# Novinky ve standardech 802.11

**Václav Moural**
**Intercom Systems a.s.**
**moural@intercomsys.cz**

# Agenda

- **802.11 PHY standardy (a, b, g)**

  Hybridní sítě (g + b) a problémy MAC vrstvy

  802.11a  a 802.11h  v Evropě a v ČR
- **IEEEE 802.11e (QoS)**
- **IEEEE 802.11i (bezpečnost)**
- **Ukázka strukturovaného komplexního řešení WLAN velkého rozsahu: Cisco SWAN**

# IEEE 802.11 - Standardy a projekty

***(task groups)***

| 802.11-1999 | PHY + MAC | 2,4 GHz, 2 Mb/s | 1999 |
|---|---|---|---|
| .11a | PHY | 5 GHz, 54 Mb/s | 1999 |
| .11b | PHY | 2,4 GHz, 11 Mb/s | 1999 |
| *.11e* | *MAC* | *QoS* | *4Q2004* |
| .11f | MAC | Roaming (IAPP) | 6/2003 |
| .11g | PHY | 2,4 GHz, 54 Mb/s | 6/2003 |
| .11h | PHY | DFS, TPC (harmonizace s ETSI) | 9/2003 |
| *.11i* | *MAC* | *bezpečnost* | *6/2004* |
| *.11k* | | *management* | *2004-5* |
| *.11n* | *PHY* | *? GHz, 108 (320) Mb/s* | *2006* |

# 802.11 PHY

| | 802.11b | 802.11g | 802.11a |
|---|---|---|---|
| Pásmo | 2,4 GHz) | 2,4 GHz | 5 GHz |
| Počet nepřekrývajících se kanálů | 3 | 3 | 8 + 10 + 4 |
| Modulační schema | (FHSS,) DSSS (rozprostřené spektrum) | OFDM | OFDM |
| Rychlosti (Mb/s) | 1, 2, 5.5, 11 | 6,9,12,18,24,36,48,54 | 6,9,12,18,24,36,48,54 |
| Max. výkon (EIRP) | 100 mW (20dBm) | 30 mW (15dBm) | 200 mW (indoor) |

# Průchodnost (throughput) sítí 802.11

| | Rychlost PHY (Mb/s) | Průchodnost (throughput) (Mb/s) | Průchodnost vztažená k 802.11b | Kapacita (průchodnost x počet kanálů) |
|---|---|---|---|---|
| 802.11b | 11 | 6 | 100% | 18 |
| 802.11g (s klienty 802.11b) | 54 | 7 | 117% | 21 |
| 802.11g (bez klietů 802.11b) | 54 | 22 | 367% | 66 |
| 802.11a | 54 | 25 | 417% | 300 |

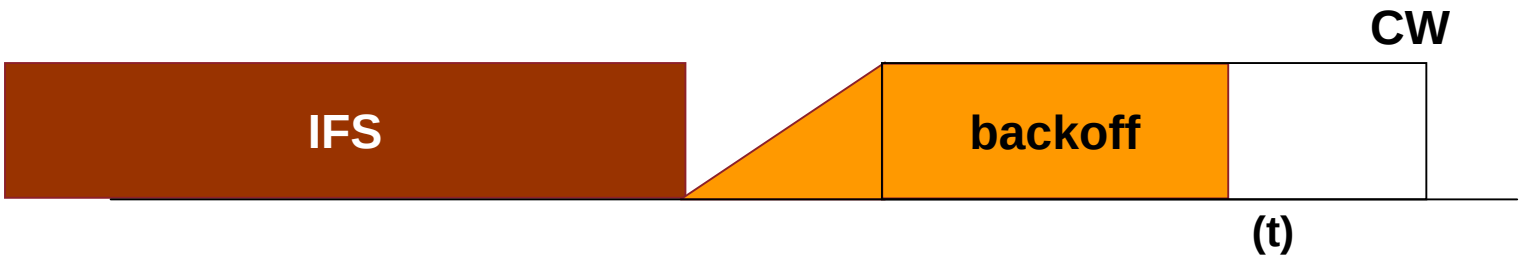
# CSMA/CA: DCF (802.11 MAC)

- **DCF: *Distributed Coordination Function***
- **V hlavičce rámce je doba rezervace media (*duration*)**
- **Každý klient podle ní nastaví své počitadlo, jak dlouho bude medium obsazené (NAV – *Network allocation vector*)**
- **Když NAV=0, začne IFS (*Inter Frame Space*) – 50㎳ pro 11.b**
- **Po IFS začne *Content Window* (Rita P.: „okno sváru“)**

  **Klient volí „*random backoff*“: náhodný počet časových slotů z CWmin, než se pokusí vysílat,**

  **11b: CWmin = 31 x 20 ㎳, 11g: CWmin = 9 x 15 ㎳**

  **Když kolize (chybí ACK) retransmise s dvojnásobným CW, dokud CW<CWmax**



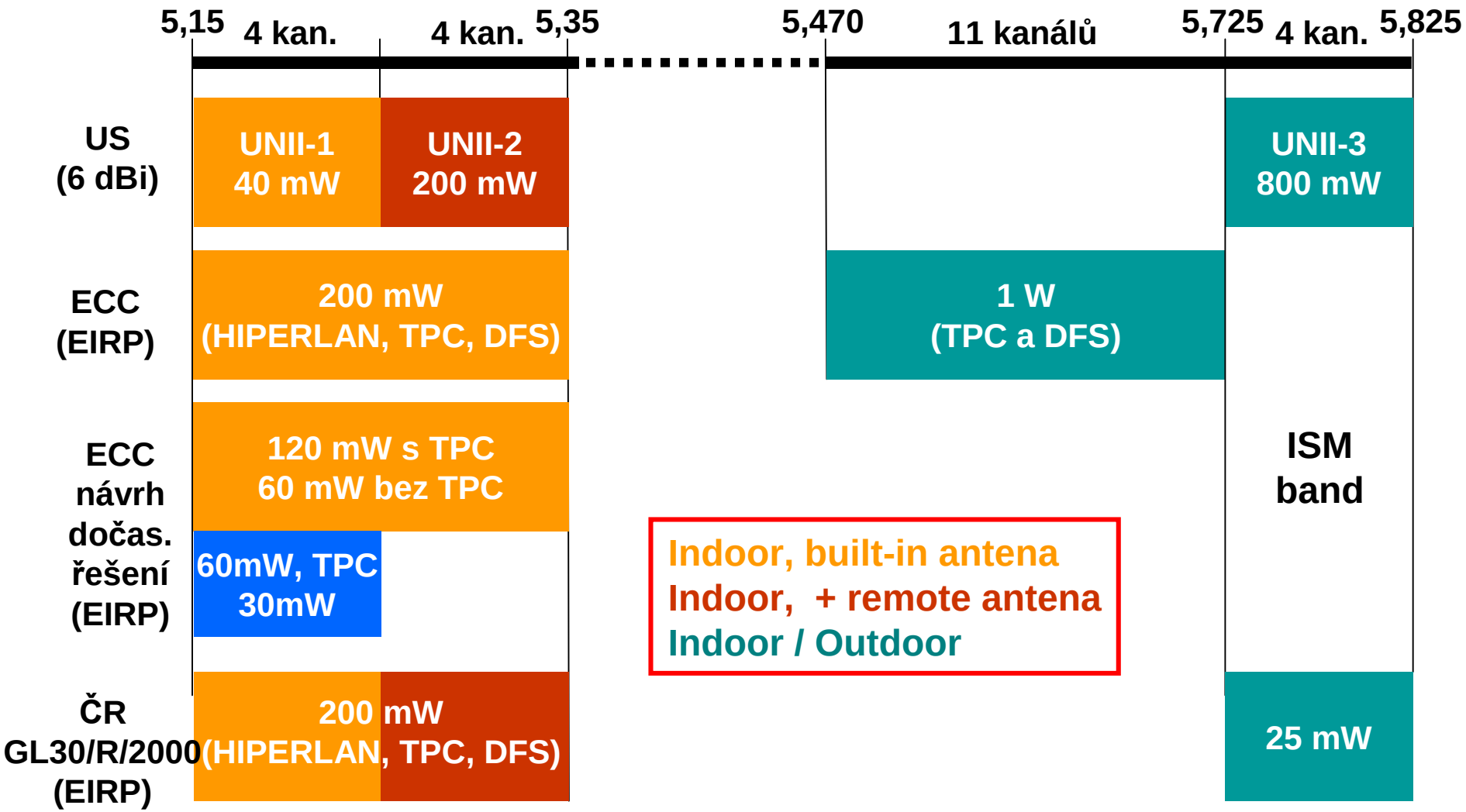
# DFC: Problém hybridní sítě 11g +11b

- **Potřeba ACK: Vysílající stanice nemůže indikovat kolizi**
- **Pro ACK a AP je IFS menší (*Short IFS*, *Point IFS*)**
- **RTS/CTS: *Request-to-Send* / *Clear-to-Send* aktivuje AP:**
  - **když je rámec delší než *threshold***
  - **když v síti jsou skrytí klienti, kteří se kvůli vzdálenosti nemohou „slyšet“**
- **11b klient „nerozumí“ 11g radiu, nenastaví NAV, CSMA/CA nefunguje**
- **AP to řeší tak, že když má 11b klienta, vnutí všem RTS/CTS**
- **11g *option*: *CTS to self* – může zvýšit průchodnost**

# Srovnání dosahu 802.11a/b/g při různých rychlostech

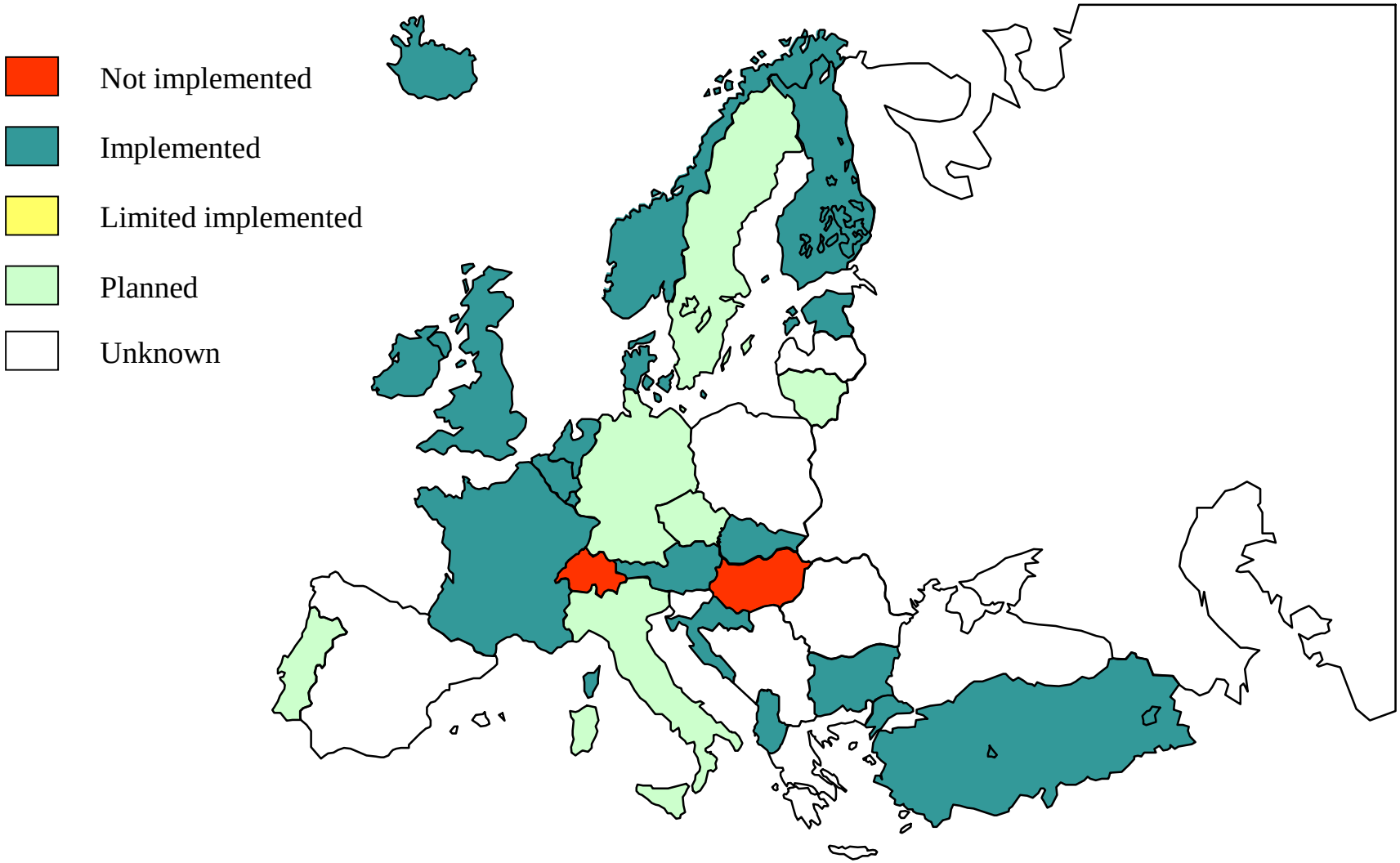
| Data Rate (Mbps) | 802.11a (40 mW with 6dBi gain diversity patch antenna) Range | 802.11g (30 mW with 2.2 dBi gain diversity dipole antenna) | 802.11b (100 mW with 2.2 dBi gain diversity dipole antenna) |
|---|---|---|---|
| 54 | 45 ft (13 m) | 90 ft (27 m) | - |
| 48 | 50 ft (15 m) | 95 ft (29 m) | - |
| 36 | 65 ft (19 m) | 100 ft (30 m) | - |
| 24 | 85 ft (26 m) | 140 ft (42 m) | - |
| 18 | 110 ft (33 m) | 180 ft (54 m) | - |
| 12 | 130 ft (39 m) | 210 ft (64 m) | - |
| 11 | - | 160 ft (48 m) | 160 ft (48 m) |
| 9 | 150 ft (45 m) | 250 ft (76 m) | - |
| 6 | 165 ft (50 m) | 300 ft (91 m) | - |
| 5.5 | - | 220 ft (67 m) | 220 ft (67 m) |
| 2 | - | 270 ft (82m) | 270 ft (82m) |
| 1 | - | 410 ft (124 m) | 410 ft (124 m) |

# 802.11a: Struktura pásma 5 GHz, omezení




GL-30: ČSN ETS 300 836-1, EN 300 220-1, EN 300 330, EN 300 440

# Stav implementace 802.11a v pásmu 5150-5350 MHz v Evropě



# ČTÚ a 802.11a v ČR

- Platí GL-30/R/2000
- V průběhu r. 2003 jednání G12 s ČTÚ
- Tel. věstník 9/2003: Návrh nové GL pro RLAN:
  - 5150-5350: uvnitř budov, EIRP 200mW5150
  - 5470-5725: uvnitř i vně, EIRP 1W, TPC, DFS
- 30.12.2003: vyčkat rozhodnutí CEPT, bude to brzy
- 20.2.2004: EK pověřila CEPT předložením návrhu aktualizovaného rozhodnutí do 6/2004, schváleno bude do 11/2004

- Závěr: Do konce roku by měla být nová GL
- Povolí provoz zařízení, která splní 802.11h (TPC a DFS) alespoň v rozsahu návrhu GL z 9/2003

- Poznámka: Dodatek GL pro pásmo 2,4 GHz povolil 802.1g teprve v dubnu 2004 (k rozprostřenému spektru přidal OFDM)

# IEEE 802.11h

- **Standard ratifikován 9/2003**
- **Rozšíření MAC vrstvy vyžadované pro 802.11a**
- **TPC: *Transmitt Power Control***

  **Automatická regulace výkonu**

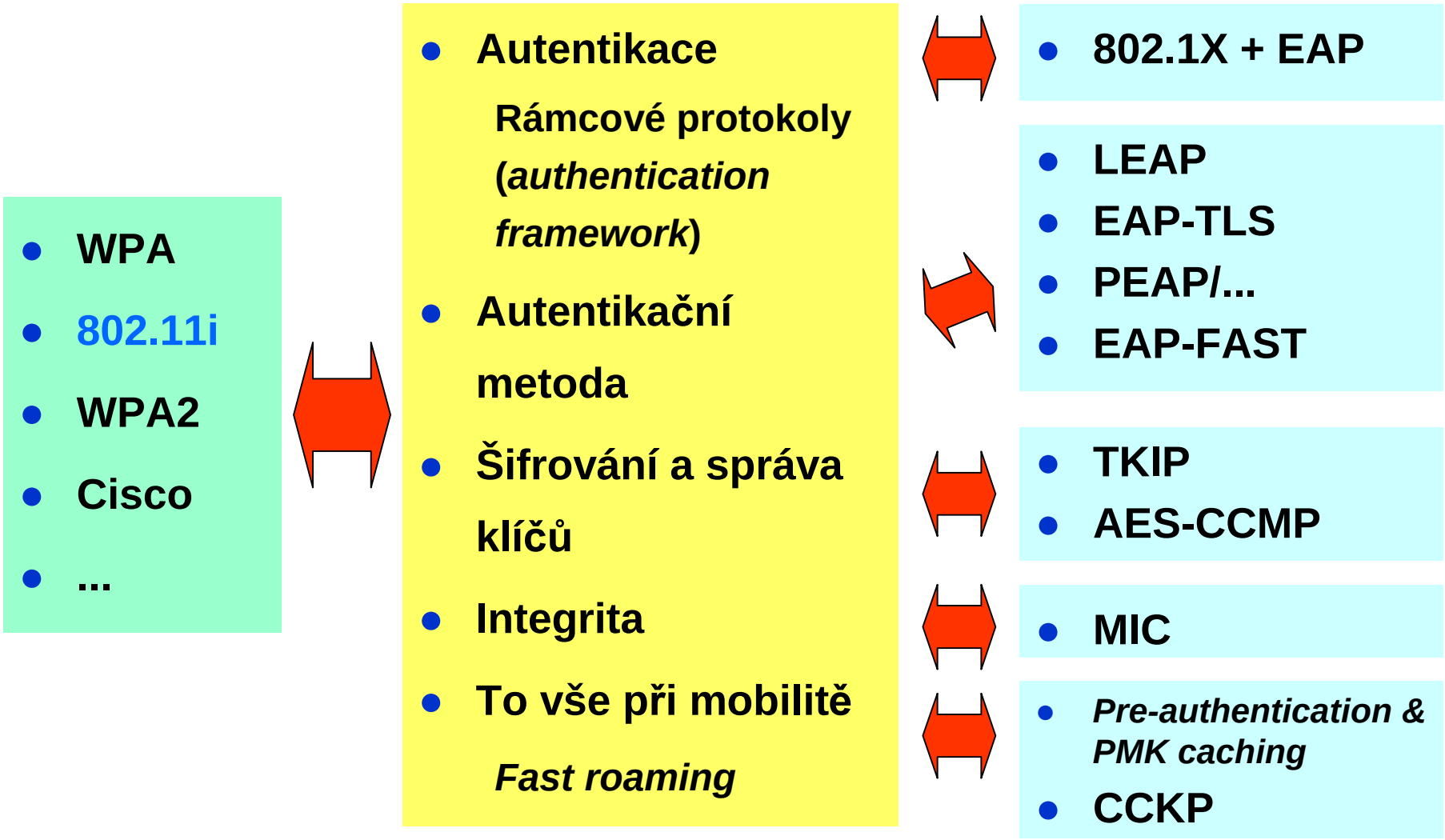
  **Implementace asi přes beacon frame, který posílá AP**
- **DFS: *Dynamic Frequency Selection***

  **Dynamická volba kmitočtu- rovnoměrné využití spektra**
- **Cisco: tvrdí, že TPC už má a DFS bude mít v září (plně v souladu s 802.11h)**

# 802.1e: QoS

- **Ratifikace 4Q2004**
- **Povinné:**
  - **Podpora 8 prioritních tříd**
  - **EDCF: *Enhanced DCF*: různým třídám provozu se přiřadí různé IFS (tzv *Arbitrary IFS* – AIFS)**
  - **Případně i různé délky CW (*Conention Window*), tj. pravděpodobnostně různě dlouhé čekání po IFS (*backoff*)**
- **Volitelné:**
  - **HCF (*Hybrid Coordination Function*) = Modifikace volitelné funkce PCF (*Point Coordination Function*) standardu 802.11, kde AP může střídat**
    - ***Contention Period* (normální CSMA/CA) s**
    - ***Cotention-free period*, kdy vyzývá stanice podle priority**
  - ***Automatic Power Save Delivery* (APSD): probouzení spících stanic**
- **WiFi Aliance: WMA – *Wireless Multimedia Access***
  - **dosud se necertifikuje, mělo by se od září současně s WPA2 (8002.11i)**
- **Cisco: pre-standard EDCF**
  - **VxWorks a 7920: diferencované CWmin a CWmax (random backoff)**
  - **IOS: diferencuje jak IFS, tak CW**

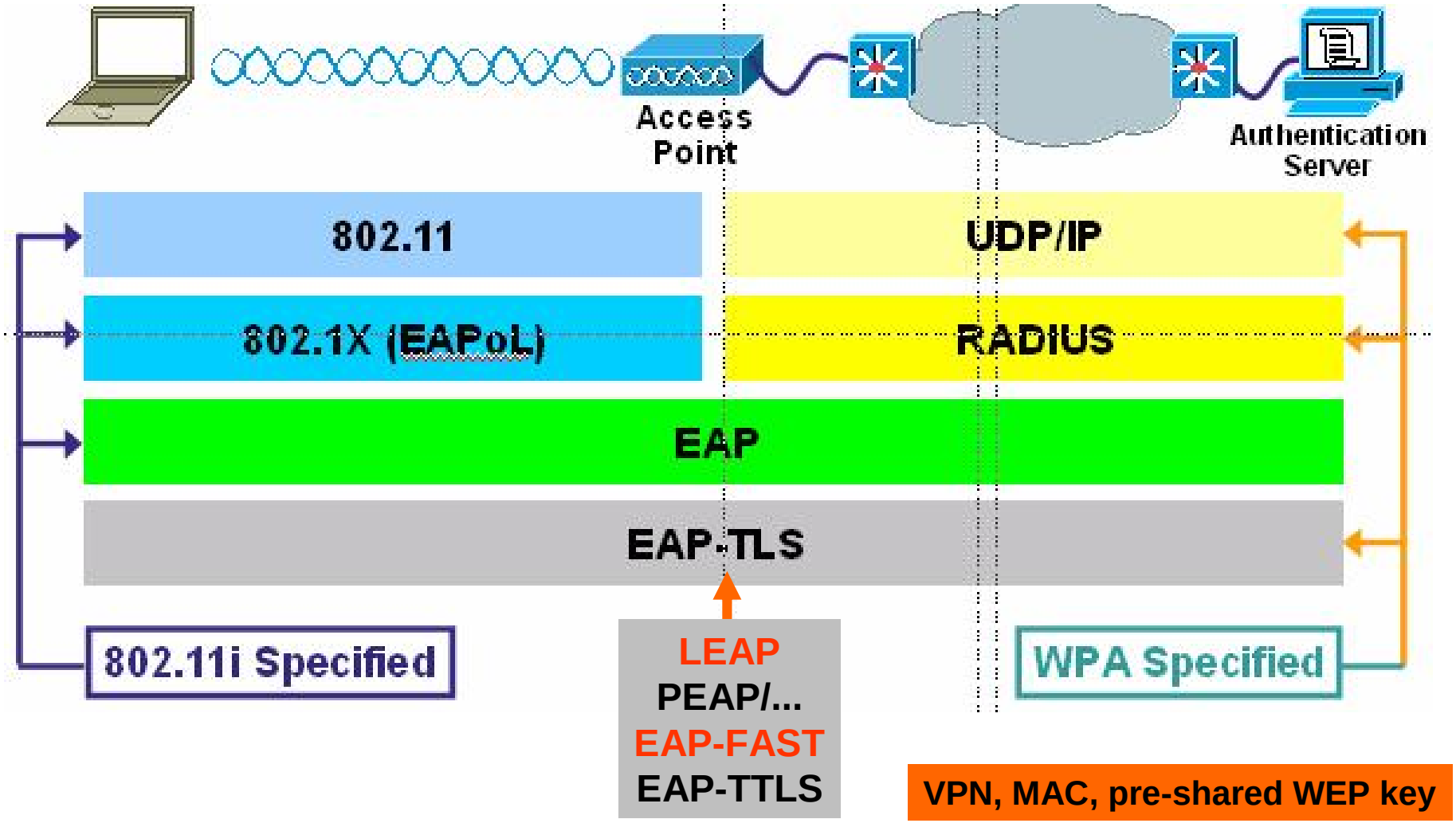
# 802.11i: Bezpečnost



# Standardizované sady protokolů

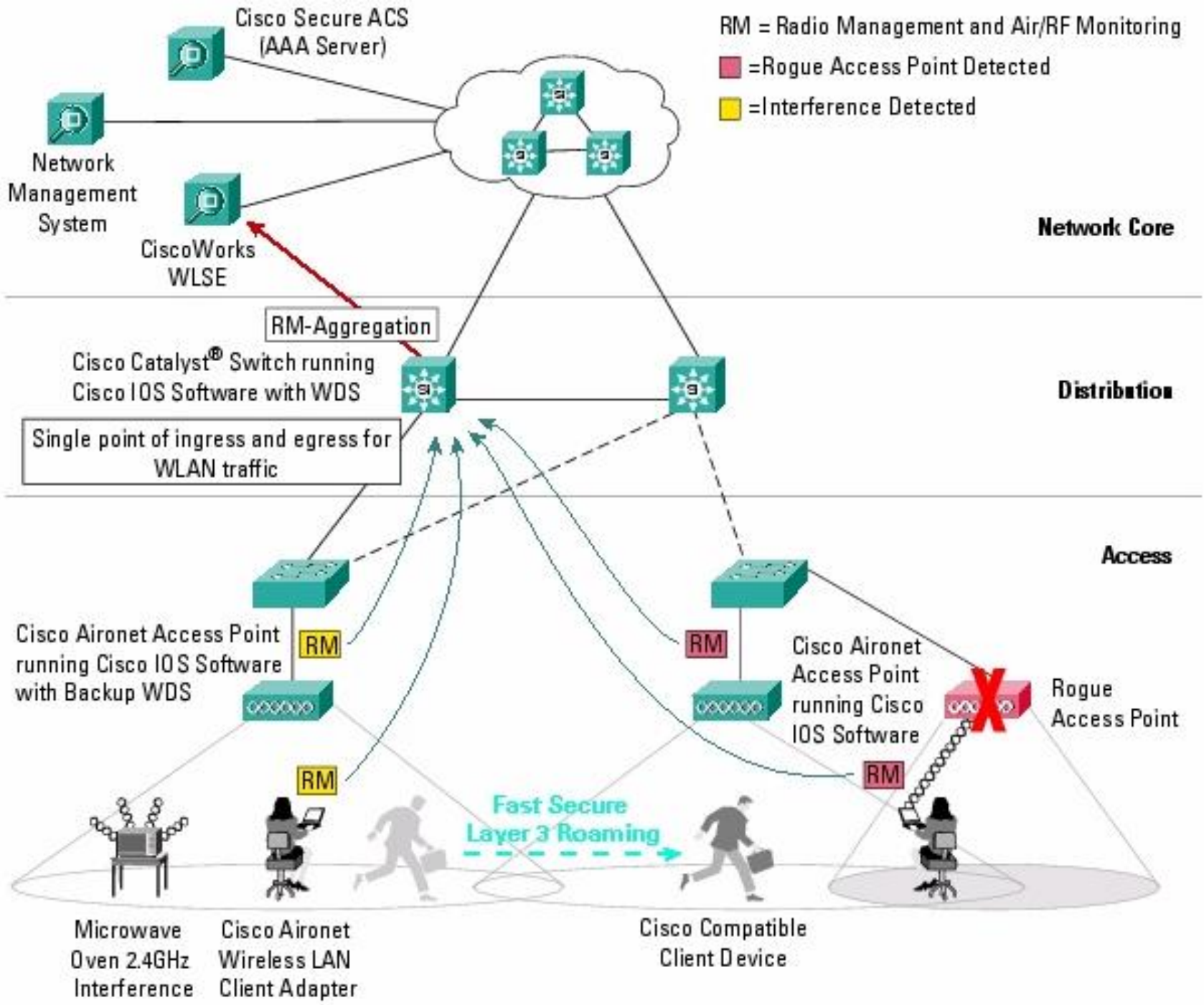
- **WPA: *WiFi Protected Access***
  - **Založen na 802.11i, Draft 3**
  - **802.1X**
  - **EAP-TLS nebo *Pre-shared Key***
  - **(WPA) TKIP**
- **TKIP – *Temporal Key Integrity Protocol***
  - ***Per-Packet Keying***
  - **MIC**
  - ***Broadcast Key Rotation***
  - **Šifrování RC4**
- **802.11i**
  - **Ratifikace 6/2004**
  - **802.1X + EAP**
  - **Nespecifikuje autentikační metodu**
  - **AES (*Advanced Encr. System*) – 128 bitová silná šifra**
  - **MIC**
  - **Pre-authentication & PMK caching (nepovinné?)**
- **WPA2: podle 802.11i (?)**

# Autentikace a její metody



# Cisco SWAN

- ***Structured Wireless-Aware Network***
- **Cíle:**
  - ***Fast Secure roaming* L2, L3 (*point-to-multipoint* GRE tunely)**
  - ***Radio Management***
  - **Centralizovaná bezpečnost**
  - **Centralizované řízení bezdrátové infrastruktury**
- Snadné ovládání řádově tisíců AP
- Zjednodušení náročných a nákladných operací:
  - ***Site surveys*, *rogue AP detection*, *interference detection and mitigation***
- Prvky:
  - **WDS (*Wireless Domain Services*) na IOS AP (mj. *ARP caching*, *local RADIUS*)**
  - **Catalyst 6500 WLSM (*Wireless Services Modul*) - HW podpora multipoint GRE tunelů**
  - **WLSE (*Wireless Services Engine*) – HW + management SW**
  - **Radius server (např. Cisco Secure ACS)**


Cisco Secure ACS
(AAA Server)
RM = Radio Management and Air/RF Monitoring
=Rogue Access Point Detected
=Interference Detected
Network
Management
System
CiscoWorks
WLSE
Network Core
RM-Aggregation
Cisco Catalyst® Switch running
Cisco IOS Software with WDS
Distribution
Single point of ingress and egress for
WLAN traffic
Access
Cisco Aironet Access Point
running Cisco IOS Software
with Backup WDS
RM
RM
RM
RM
Cisco Aironet
Access Point
running Cisco
IOS Software
Rogue
Access Point
Fast Secure
Layer 3 Roaming
Microwave
Oven 2.4GHz
Interference
Cisco Aironet
Wireless LAN
Client Adapter
Cisco Compatible
Client Device

# IEEE 802.16

- Broadband Wireless Access WG
- WirelessMAN Air Interface
- 802.16: 10- 60 GHz, přímá viditelnost, 50 km
- 802.16a: 2-11 GHz, NLOS , 70Mb/s P2P, 384 kb/s edge
- 802.16e: mobility (do 150 km/h), 2-6 GHz, NLOS
- Point-to-multipoint, mesh topologie
- TDM, TDMA, TDD i FDD
- Connection oriented
- Convergence Layer
- Adaptivní modulace a kódování
- Je to G4?
- http://wirelessman.org

# IEEE 802.16

- **WiMAX: http://wimaxforum.org**

  Airspan, **Alvarion**, Hughes Network Systems,
  Ensamble Communications, **Fujitsu**, **Intel**, **Nokia**, OFDM Forum,
  Telnecity Group, Proxim
- **Intel chipset (?)**
- **Očekává se „rozjezd“ rychlejší než u WiFi**
- **1 bn $ do roku 2008**
- **Max. boom v roce 2006**

# IEEE 802.20

- MBWA, Mobile Broadband Wireless Access
- Flarion (Cisco), Motorola
- Standard (draft) by měl být do konce roku
- Do 250 km/hod
- Pásmo < 3,5 GHz
- Rychlost > 1 Mb/s upstream, 300 kb/s downstream
- patrně několik vrstev
- Kombinace FDD a TDD (Frequency/Time Division Duplex)
- Průměr dosahu buňky cca 15 km
- AES
- Konkurence s 802.16e?