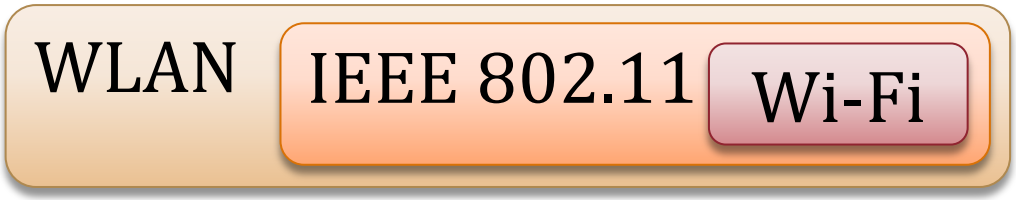
Lekce 6: sítě WLAN II

Jiří Peterka

Wi-Fi, certifikace

- **WLAN (Wireless LAN) je obecné označení pro všechny bezdrátové sítě LAN**
  - dnes nejrozšířenější jsou takové sítě, které vychází ze standardů IEEE 802.11
    - ale existují i jiné bezdrátové sítě LAN, např. HiperLAN, HomeRF .....



- **Wi-Fi (od: Wireless Fidelity) je „nálepka“, vyjadřující získání certifikace o:**
  - dodržení standardů IEEE 802.11
  - interoperabilitě s ostatními produkty dle standardů IEEE 802.11
- **„nálepku“ Wi-Fi uděluje sdružení Wi-Fi Alliance**
    - dříve: sdružení **WECA** (Wireless Ethernet Compatibility Alliance)
  - uděluje ji konkrétním produktům od konkrétních výrobců
    - poté, co tyto produkty úspěšně projdou testováním v nezávislých odborných laboratořích
      - které Wi-Fi Alliance autorizuje (a které testují podle její metodiky a kritérií)
    - výsledky testování lze nalézt v databázi Wi-Fi Alliance (http://www.wi-fi.org/product-finder)
  - certifikuje se vůči různým profilům (programům), které se týkají dílčích standardů
      - a tím i konkrétních schopností, funkcí, vlastností atd.
    - např. podpory standardů 802.11b/g/n/ac, WPA, WPA2 atd.

http://www.wi-fi.org/

ne všechny produkty, které se prezentují jako Wi-Fi, jsou certifikovány a mají právo nosit „nálepku Wi-Fi“ !!!

příklad konkrétního produktu

Consumers & Retailers START HERE

The worldwide network of companies that brings you Wi-Fi®

počet certifikovaných produktů v databázi

SHOW NAVIGATION

Product Finder

Your Search Results (22179) Start new search

Clear all filters

Keyword Search ADD

Manufacturer

Categories

- Computers & Accessories (4545)
- Gaming, Media & Music (1107)
- Phones (4722)
- Routers (6228)
- Smart Home (36)
- Tablets, Ereaders & Cameras (1036)
- Televisions & Set Top Boxes (4850)
- Other (1119)

Featured Capabilities

- Passpoint™ (799)
- Miracast® (3470)
- Wi-Fi Direct® (6859)
- Wi-Fi CERTIFIED™ ac (1071)
- Wi-Fi CERTIFIED™ n (16815)
- Voice-Enterprise (66)
- Wi-Fi Protected Setup™ (12716)

Show Advanced Filters

Samsung Galaxy Note 4 (SM-N910F) Charcoal Black

26x 517

výčet profilů, vůči kterým je daný produkt certifikován

http://www.wi-fi.org/product-finder

Product Details

SAMSUNG ELECTRONICS

Certification ID: WFA55732

Date of Last Certification: 2014-09-02
Manufacturer: Samsung Electronics
Product: SM-N910F
Model Number: SM-N910F
Category: Smartphone, multi-mode (Wi-Fi and other)
Hardware Version: REV1.1
Firmware Version: REV1.0
Operating System: Android
Frequency Band(s): 2.4 GHz, 5 GHz

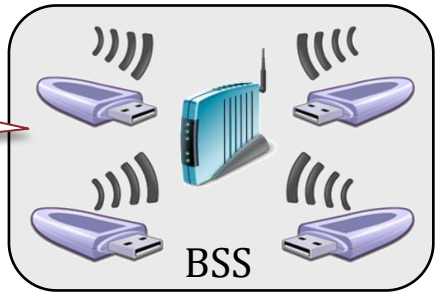
Summary of Certifications

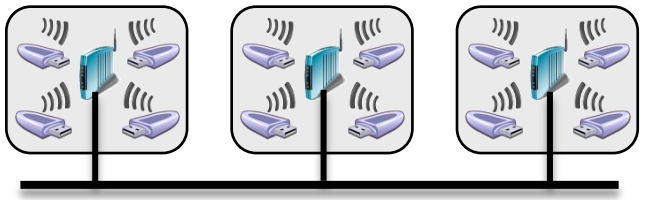
CLASSIFICATION	PROGRAM
Connectivity	Wi-Fi CERTIFIED™ b
	Wi-Fi CERTIFIED™ a
	Wi-Fi CERTIFIED™ g
	WPA™ - Enterprise
	WPA™ - Personal
	WPA2™ - Enterprise
	WPA2™ - Personal
	Wi-Fi CERTIFIED™ n
	Wi-Fi Direct®
	Wi-Fi CERTIFIED™ ac
Optimization	WMM®
	WMM®-Power Save
Access	Wi-Fi Protected Setup™
	Passpoint™ (Release 1)
Applications & Services	Miracast - Source

systémová architektura 802.11

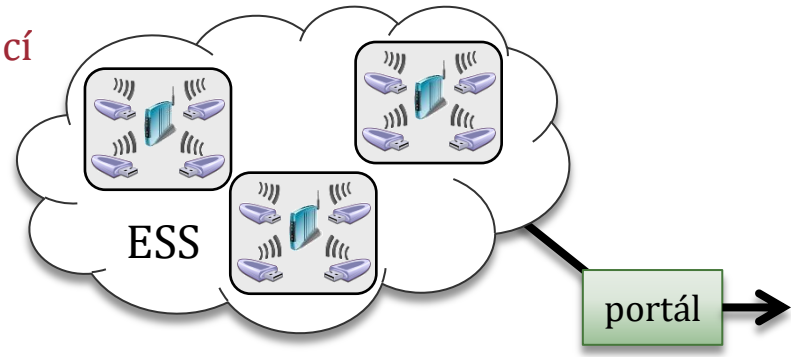
- **má následující prvky:**
  - (koncové) **stanice**: **STA**
    - uzly, vystupující v roli koncových stanic
  - **přístupový bod**: **AP** (Access Point)
    - uzly, vystupující v roli přístupových bodů
  - **buňka**: **BSS** (Basic Services Set)
    - základní jednotka infrastruktury
      - může fungovat ve dvou různých režimech
        - v režimu infrastruktury má 1 přístupový bod (AP) a několik stanic (STA)
        - v režimu ad-hoc nemá žádný přístupový bod
      - každá buňka má svůj jednoznačný identifikátor: **BSSID**
  - **distribuční systém**: **DS** (Distribution System)
    - zajišťuje vzájemné propojení dvou či více buněk (BSS)
  - **síť**: **ESS** (Extended Services Set)
    - několik buněk (BSS), propojených mezi sebou pomocí distribučního systému (DS)
    - každá síť má svůj jednoznačný identifikátor: **ESSID**
  - **portál**
    - zajišťuje propojení sítě (ESS) s jinými sítěmi LAN

jde o obdobu segmentu v drátových sítích



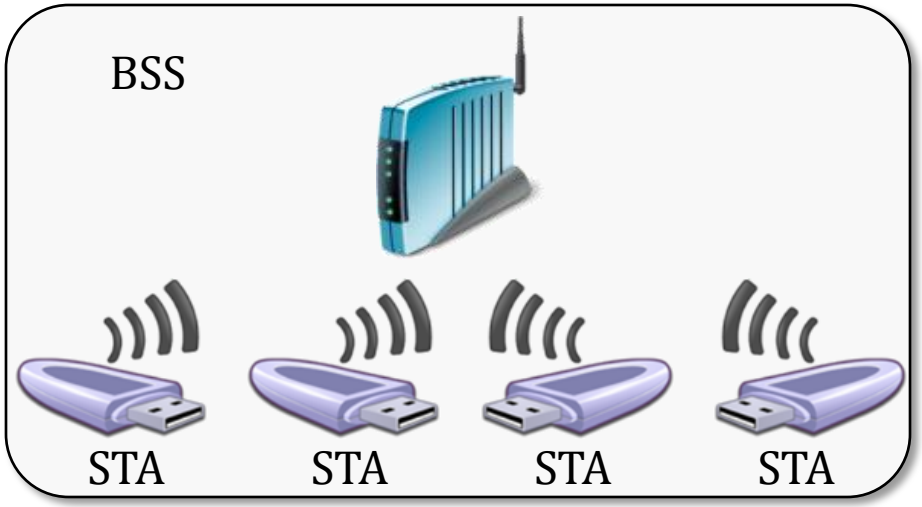


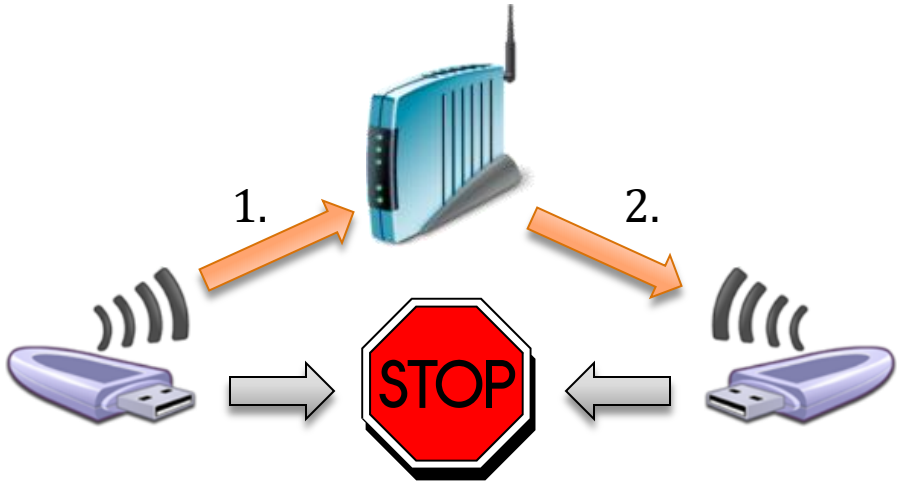
DS: Distribution System



BSS, Basic Services Set (buňka)

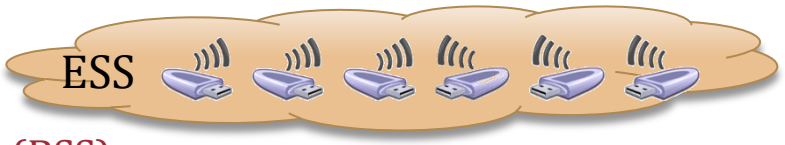
- **jde o základní prvek infrastruktury sítí dle standardu IEEE 802.11**
  - odpovídá segmentu u „drátových“ sítí
    - přesněji: kolizní doméně v Ethernetu – všechny uzly v BSS společně sdílí dostupnou kapacitu!!
      - je podobná buňce v mobilních sítích
  - funguje v **režimu infrastruktury**
    - tj. má 1 přístupový bod (AP) a jednu či více stanic (STA)
      - v rámci přístupové metody DCF mají všechny uzly (AP i STA) stejné postavení
        - pouze v rámci PCF má výsadní postavení AP, které se dotazuje jednotlivých stanic
    - stanice v BSS spolu nekomunikují přímo, ale jen přes AP !!!
      - když jedna stanice (STA1) potřebuje něco poslat jiné stanici (STA2) ve stejné BSS, pošle to nejprve přístupovému bodu (AP), a ten to následně předá druhé stanici (STA2)
        - v rámci BSS probíhá vždy nejvýše jedna komunikace (a to od/k přístupovému bodu)

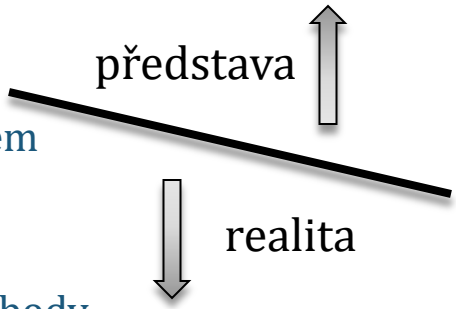


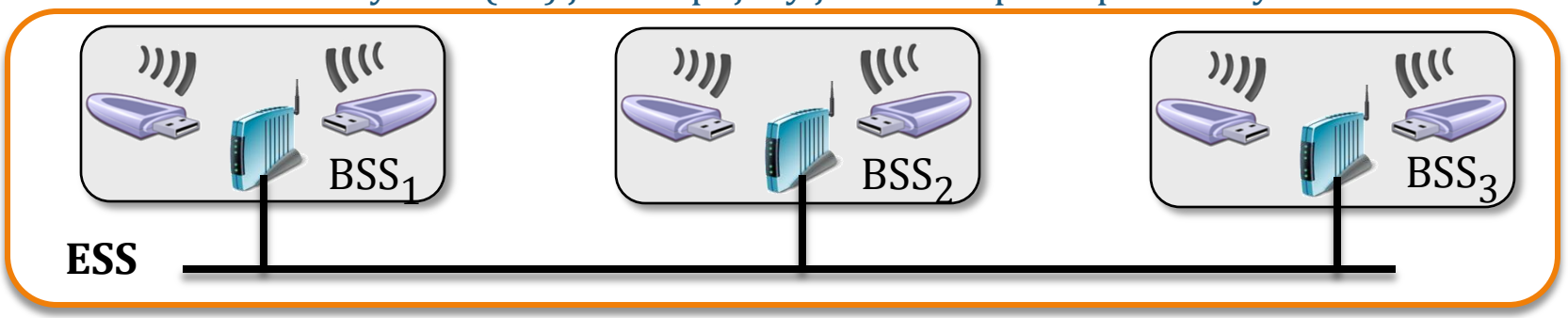


ESS, Extended Services Set (síť)

- **ESS je „vyšší“ prvek infrastruktury sítí dle standardu IEEE 802.11**
  - odpovídá síti (u „drátových“ sítí)
    - celku, propojenému na úrovni linkové vrstvy (L2)
    - má vlastní identifikátor: **SSID** (32-znakový řetězec)
  - všechny stanice (STA) v ESS jsou „jakoby: na jedné hromadě“
    - mohou si myslet, že patří „do stejného oblaku“ a mají přímé (L2) spojení mezi sebou
      - obdobně, jako uzly „drátových“ sítí
  - ve skutečnosti je to ale jinak:
    - jednotlivé stanice (STA) patří do konkrétních buněk (BSS)
      - každá stanice může „patřit“ jen do jedné buňky (BSS)
    - v každé buňce je jeden přístupový bod (AP)
      - a každá stanice v BSS komunikuje jen s tímto přístupovým bodem
    - jednotlivé BSS jsou vzájemně propojeny (do výsledného ESS) prostřednictvím distribučního systému (DS)
      - na distribuční systém (DS) jsou napojeny jednotlivé přístupové body

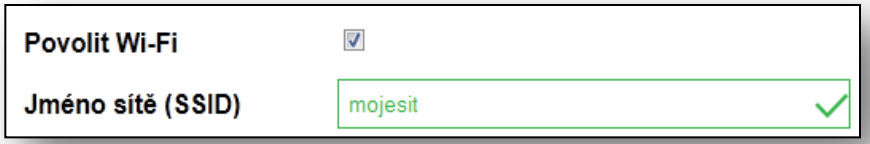




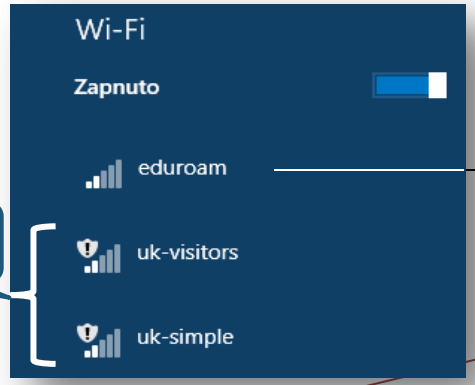


identifikátory

- **SSID** (32 znaků) je „jméno sítě“
  - někdy označováno též jako ESSID
  - identifikátor ESS
    - je společný pro všechny buňky v síti
      - pro všechny BSS v ESS
  - tento identifikátor nastavuje správce sítě, podle svého uvážení

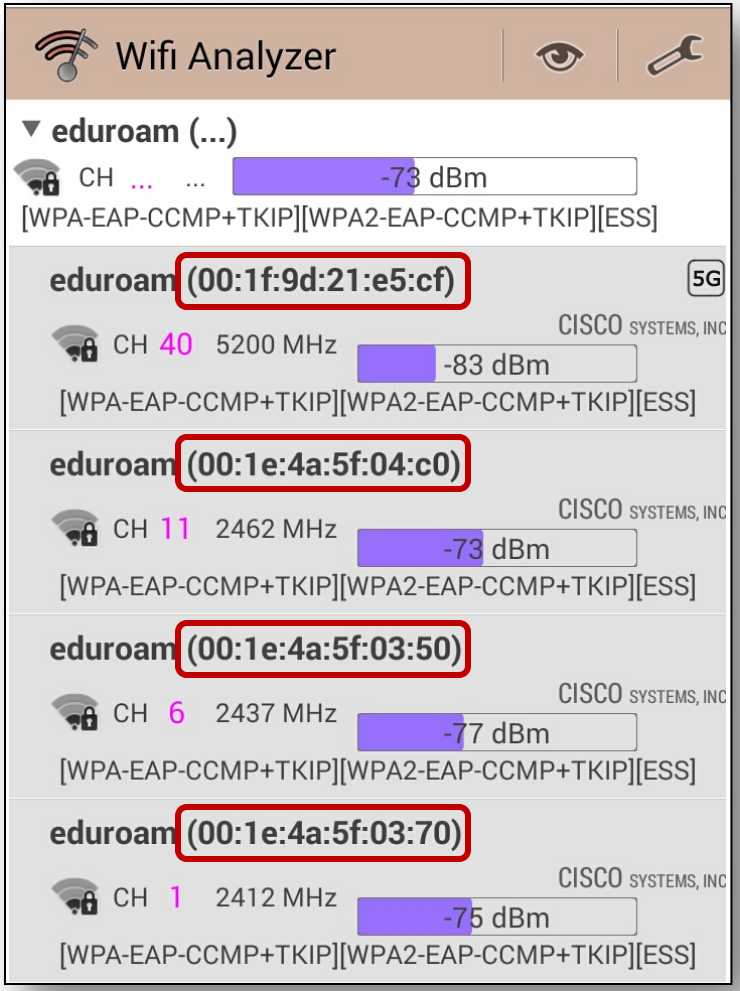


  - zobrazuje se při hledání sítí WLAN



nezabezpečené sítě

- **BSSID** (6 bytů) je identifikátor buňky
  - identifikátor BSS
  - jde o MAC adresu přístupového bodu
    - BSSID zobrazují jen specializované programy

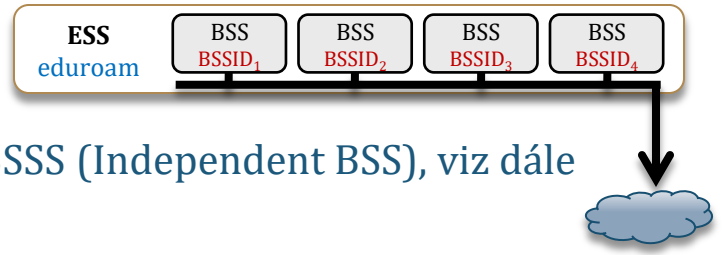


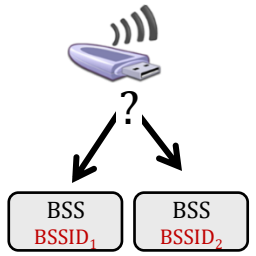
SSID

$BSSID_1$ až $BSSID_4$

DS, Distribution System

- **DS (distribuční systém) je nutný kvůli tomu, aby bylo možné:**
  - napojit buňku (BSS) na „okolí“
    - aby buňka nebyla zcela izolovaná od vnějšího světa
      - existují i izolované buňky (bez napojení na okolí): IBSSS (Independent BSS), viz dále
  - „spojit“ více buněk (BSS) do jedné sítě (ESS)
    - a bylo možné vytvářet iluzi, že všechny stanice v síti (ESS) jsou “jakoby na jedné hromadě“
  - realizovat agendu, spojenou se strukturou sítí a příslušností jednotlivých stanic (STA) do konkrétních buněk (BSS)
    - které buňky tvoří síť? Které uzly jsou jejich přístupovými body?
    - když zde „nejsou dráty“, jak se pozná, do které buňky patří konkrétní stanice?
  - zajišťovat přenos dat v rámci buněk, mezi buňkami i z/do sítě





- **standardy IEEE nedefinují způsob implementace DS !!!!**
  - ale definují služby, které má DS zajišťovat !!!
    - **Station Services (SS)**
      - týkají se vazby mezi AP a STA v rámci buňky
      - Authentication (autentizace)
      - Deauthentication (de-autentizace)
      - Privacy (zajištění důvěrnosti přenášených dat)
      - MAC Service Data Unit (MSDU) Delivery
        - vlastní přenos dat mezi STA a AP
    - **Distribution System Services (DSS)**
      - týkají se příslušnosti stanic do buněk
      - Association (asociace STA k AP)
      - Reassociation (další asociace …)
      - Disassociation (zrušení asociace)
      - Distribution (přenos mezi BSS)
      - Integration (přenos do jiných sítí)

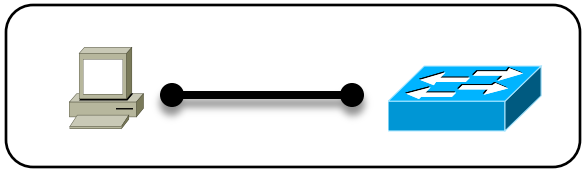
DSS: Association, Deassociation

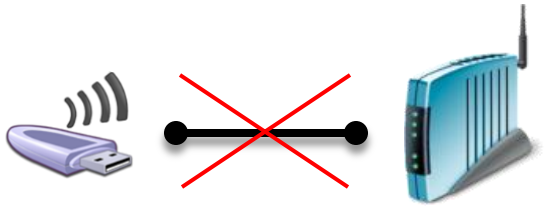
- **proč je nutná asociace (a de-asociace)?**
  - u „drátových“ sítí o příslušnosti uzlu ke konkrétnímu segmentu či síti rozhoduje jeho připojení („*vedení drátu*“)
    - u bezdrátových sítí to ale takto fungovat nemůže
      - *mezi přístupovým bodem (AP) a stanicemi (STA) nevedou žádné dráty ….*
  - u bezdrátových sítí je nutná „vzájemná domluva“ mezi stanicí (STA) a přístupovým bodem (AP) konkrétní buňky
- **jak probíhá „domluva“ na zařazení do buňky?**
  - stanice (STA) musí být v dosahu signálu přístupového bodu (AP) konkrétní buňky (BSS)
    - dosah se označuje jako BSA (Basic Set Area)

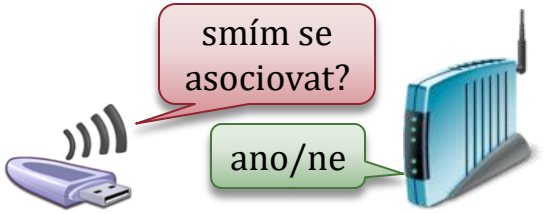
1. stanice požádá přístupový bod o „členství“ v BSS
   - STA pošle AP žádost o asociaci (DSS: **Association**)
2. přístupový bod žádosti o asociaci vyhoví
   - AP pošle STA kladné vyrozumění o asociaci

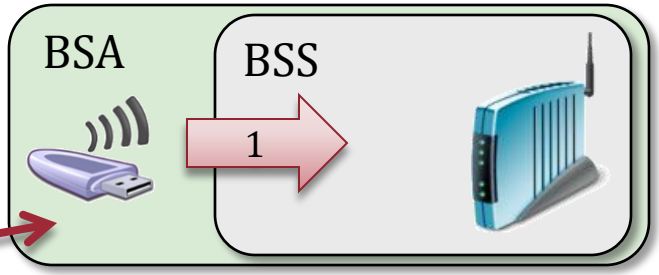
nebo ji zamítne

- **obdobně probíhá i vyřazení z buňky**
  - pomocí žádosti o zrušení asociace (DSS: **Deassociation**)



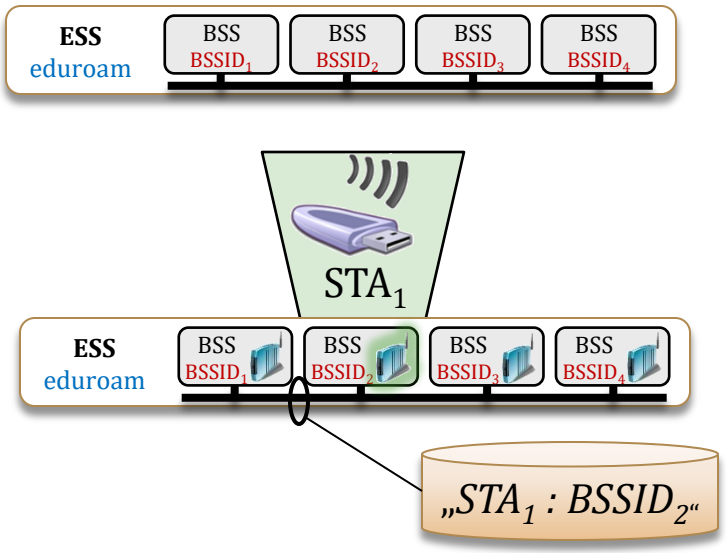




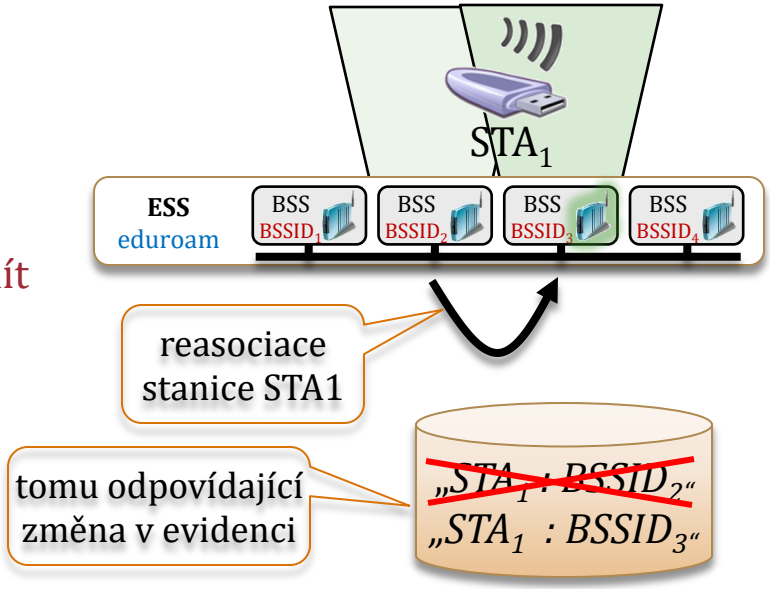


DSS: Reassociation

- **připomenutí:**
  - jedna síť (ESS) může mít více buněk (BSS)
    - propojených pomocí distribučního systému (DS)
  - stanice (STA) se asociuje vždy k „nejlepší“ buňce (BSS)
    - resp. k jejímu přístupovému bodu (AP)
      - „nejlepší“ na základě podmínek pro přenos
        - dosahu, síly signálu, nejméně rušení atd.

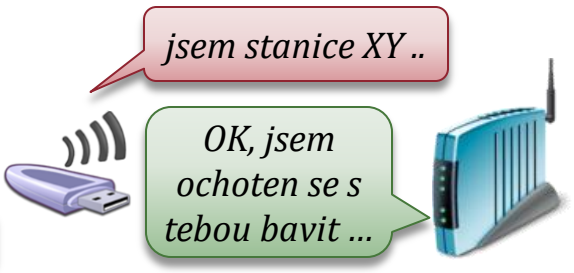


- **důsledek:**
  - distribuční systém (DS) si musí vést určitou formu evidence (databázi) toho, *„kde se která stanice nachází“*
    - se kterým AP ve které buňce je stanice asociována
- **otázka:**
  - co když se podmínky změní?
    - například když se stanice (STA) přemístí a bude mít lepší podmínky pro komunikaci s jiným přístupovým bodem (AP) v jiné buňce téže sítě?
  - pak by mělo dojít ke změně asociace
    - pomocí služby DSS: **Reassociation**
      - pro změnu asociace v rámci téže sítě (ESS)



SS: Authentication

- **kdy může přístupový bod (AP) vyhovět žádosti o asociaci?**
  - když ví, kdo (která stanice, STA) ho o asociaci žádá!
    - teprve pak se může rozhodovat
      - zda novou stanici „pustí“ do své buňky, či nikoli



- **proto je nutná autentizace**

autentizuje se stanice, nikoli uživatel !!

  - coby ověření identity té stanice, která se chce asociovat
  - stanice (STA) musí být v dosahu signálu (BSA) přístupového bodu (AP) konkrétní buňky (BSS)

1. stanice pošle přístupovému bodu žádost o (svou) autentizaci (SS: Authentication)
   - spolu s dalšími údaji, které osvědčují identitu stanice
     - např. sdílený klíč

autentizuje se pouze stanice vůči AP, naopak nikoli !!

2. přístupový bod odpoví kladně
   - pokud se mu podařilo úspěšně autentizovat stanici
     - nebo odpoví záporně, pokud autentizace nebyla úspěšná

- **původní standard 802.11 definoval 2 varianty autentizace**
  - novější standardy možnosti autentizace rozšiřují (MAC address, 802.1X, WPA, WPA2, viz dále)

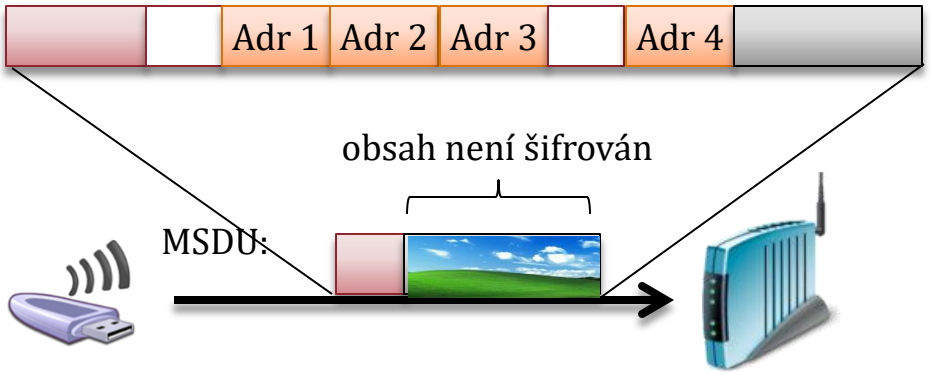
- **Open System Authentication**
  - „prázdná“ autentizace
    - přístupový bod vyhoví každé žádosti
      - a nic neposuzuje, na nic se neptá

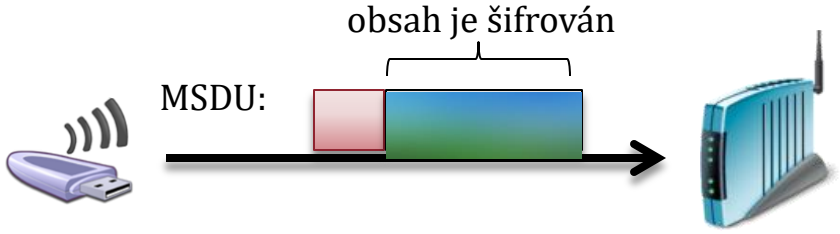
- **Shared Key Authentication**
  - skrze znalost tajného (sdíleného) klíče
    - implementováno pomocí technologie WEP (Wired Equivalent Privacy)

původně jen volitelné

SS: Delivery a Privacy

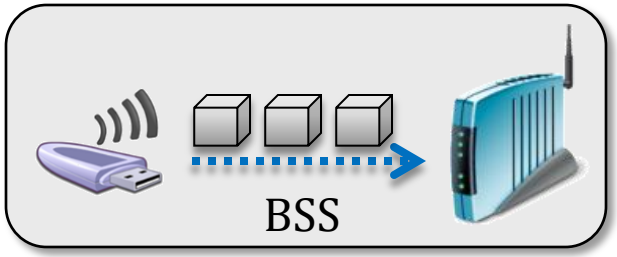
- **další služby ze skupiny SS (Station Services)**
  - **Delivery**: přenos dat mezi stanicí (STA) a přístupovým bodem (AP)
    - v podobě bloků MSDU (MAC Service Data Unit)
      - fakticky jde o přenos linkových (MAC) rámců
      - tyto rámce jsou specifické pro bezdrátové sítě na bázi standardů 802.11
        - jsou „příbuzné“ s rámci Ethernetu (802.3), ale nejsou totožné – viz dále
        - např. obsahují až 4 MAC adresy (zatímco rámce 802.3 obsahují jen 2 MAC adresy)
  - **Privacy**: (volitelné) zajištění důvěrnosti přenášených dat
    - vhodné kvůli možnosti snadného odposlechu dat přenášených bezdrátově („otevřeným prostorem“)
    - zajišťuje se šifrováním přenášených dat
      - obsahu MAC rámců (MSDU)
    - původní standard IEEE 802.11 nabízel pro šifrování (zajištění důvěrnosti) pouze technologii **WEP** (Wired Equivalent Privacy)
      - která dnes již ale není dostatečně silná
    - novější standardy nabízí další, bezpečnější možnosti
      - silnější možnosti šifrování ….



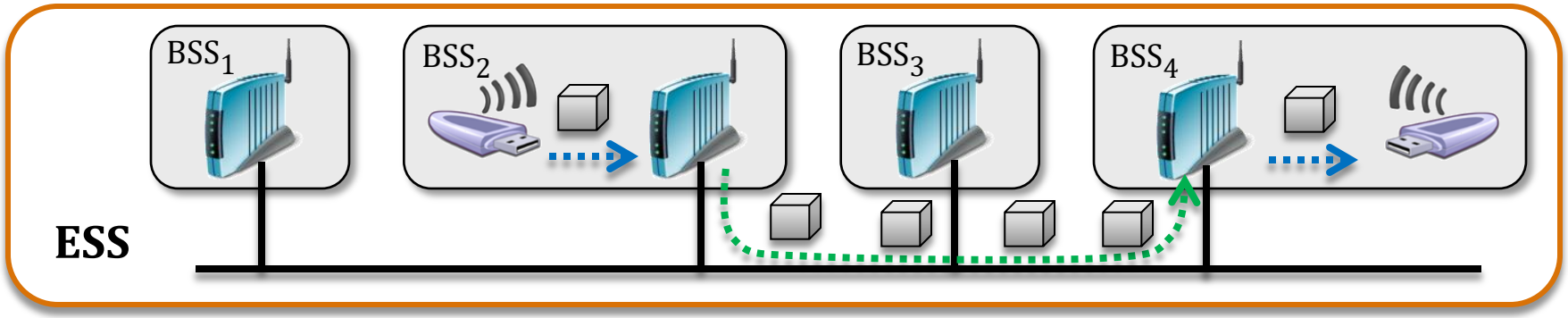


DSS: Distribution

- **služba Delivery**
  - je součástí služeb SS (Station Services)
    - protože se týká přenosu dat jen v rámci buňky (BSS)
      - mezi stanicí (STA) a přístupovým bodem (AP)
    - nemusí řešit „*kde se kdo nachází*“

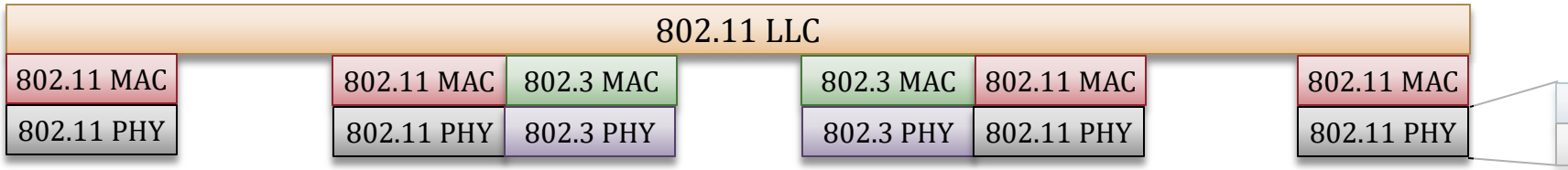


- **služba Distribution**
  - týká se přenosu i mezi buňkami (BSS)
    - proto již musí řešit, „*kde se kdo nachází*“
      - potřebuje mít informace o tom, kde se nachází zdrojová i cílová stanice (STA)
        - a z toho si odvodit, přes které přístupové body (AP) musí data projít
      - takovéto informaci má a udržuje distribuční systém (DS)
        - získává je na základě asociací/deasociací/reasociací
          - k přístupovým bodům v jednotlivých buňkách
  - proto je tato služba součástí služeb DSS (Distribution System Services)



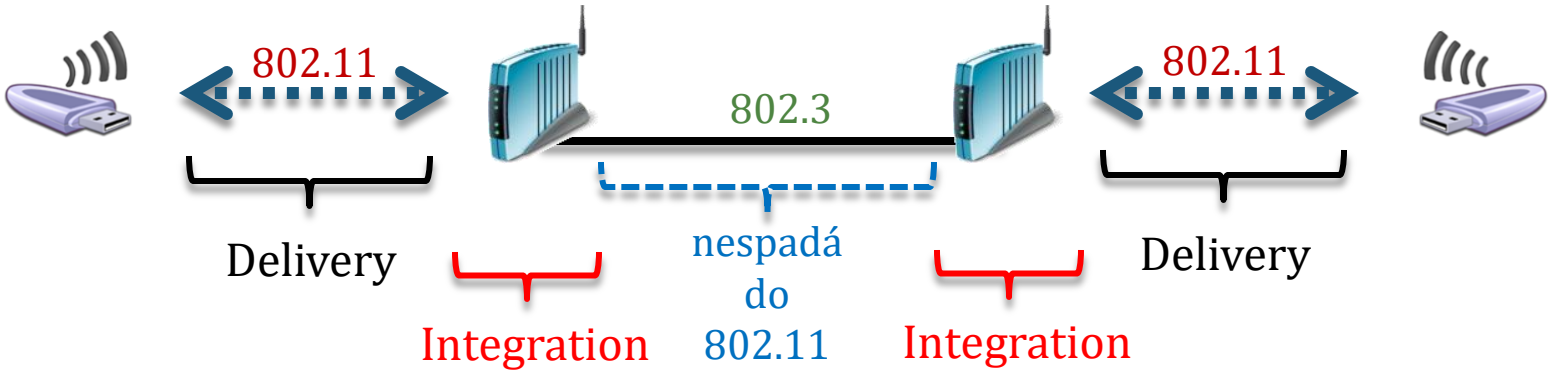
Jak je realizován distribuční systém?

- **připomenutí:**
  - standardy IEEE 802.11 nedefinují, jak má být distribuční systém (DS) implementován
    - ale definují služby, které má distribuční systém zajišťovat
      - funkce DSS: Association, Reassociation, Disassociation, Distribution, Integration
- **v praxi (obvykle):**
  - distribuční systém (DS) je realizován propojením přístupových bodů (AP) pomocí klasického „drátového“ Ethernetu (dle IEEE 802.3)
    - představa: přístupový bod má 2 rozhraní a „mezi nimi“ se chová jako přepínač
      - jedno rozhraní je bezdrátové (802.11), druhé je „drátové“ (802.3)
    - důsledek: pokud MAC rámec prochází skrz přístupový bod, je překládán z/do „bezdrátového“ formátu (dle 802.11) a „drátového“ formátu (dle 802.3)
      - zatímco vložený obsah (LLC rámec) zůstává beze změny
  - služby distribučního systému (DSS) zajišťují jednotlivé přístupové body (AP)
    - ve vzájemné součinnosti



DSS: Integration

- **připomenutí:**
  - mezi služby distribučního systému (DSS, DS Services) patří služba Delivery
    - pro (bezdrátový) přenos mezi stanicí a přístupovým bodem (v rámci buňky)
      - využívá MAC rámce 802.11
  - samotný (drátový) distribuční systém používá MAC rámce 802.3
    - které se liší od rámců 802.11
- **důsledek:**
  - musí existovat další služba distribučního systému (DSS): **Integration**
    - umožňuje provázat (propojit) bezdrátové sítě dle IEEE 802.11 s jinými sítěmi
      - hlavně se sítěmi IEEE 802.3 („drátovým“ Ethernetem)
      - *integrovat je* do jednoho celku
    - hlavní úkol služby: převod mezi MAC rámci 802.11 a jinými (obvykle MAC rámci 802.3)



MAC rámce 802.11

- **bezdrátové sítě dle standardu IEEE 802.11 používají 3 druhy MAC rámců**

1. **řídící MAC rámce** (Control Frames), slouží potřebám řízení přístupu
   - rámce pro zprávy RTS/CTS (řešení problému předsunuté a skryté stanice)
   - rámce pro zprávy ACK (potvrzování přijatých datových rámců)
2. **MAC rámce pro správu** (Management Frames)
   - Beacon rámce ("maják")
     - využívá je přístupový bod (AP) k inzerování své přítomnosti a svých parametrů
   - Probe, Probe Response
     - rámce pro zjišťování přítomnosti a schopnosti uzlů (stanic i přístupových bodů)
   - Authentication, De-authentication
     - rámce pro žádost o autentizaci/ukončení autentizace

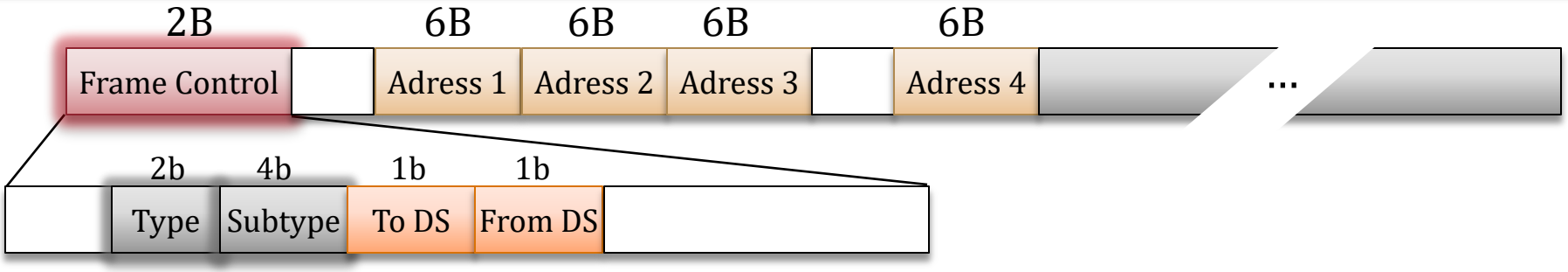
rámce Class 1

rámce Class 2

lze používat až po úspěšné autentizaci

   - Association Request/Response
     - rámce pro žádost/odpověď na asociaci
   - Re-association Request/Response
     - rámce pro žádost/odpověď na asociaci stanice (STA) s přístupovým bodem (AP) v jiné buňce (BSS) téže sítě (ESS)
   - Disassociation
     - rámec pro žádost o ukončení asociace stanice (STA) s AP
3. **datové MAC rámce**
   - pro vlastní přenos dat

formát MAC rámců 802.11



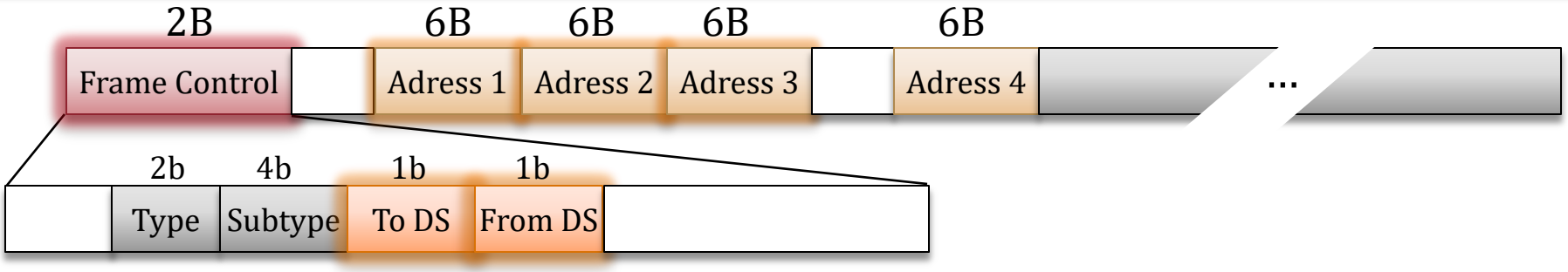
- **Frame Control:**
  - „hlavní část“ hlavičky MAC rámce, obsahuje údaje o typu rámce
    - **Type**: zda jde o řídící rámec (00), rámec pro správu (01) nebo datový rámec (10)
    - **Subtype**: detailnější rozlišení typu rámce pro jednotlivé kategorie

Type=00
- 0000: Association Request (žádost o asociaci), 0001: Association Response (odpověď)
- 0100: Probe Request („dotaz“, viz dále), 0101: Probe Response
- 1000: Beacon („vysílání majáku“, viz dále)
- 1011: Authentication (žádost o autentizaci), 1100: Deauthentication
- …….

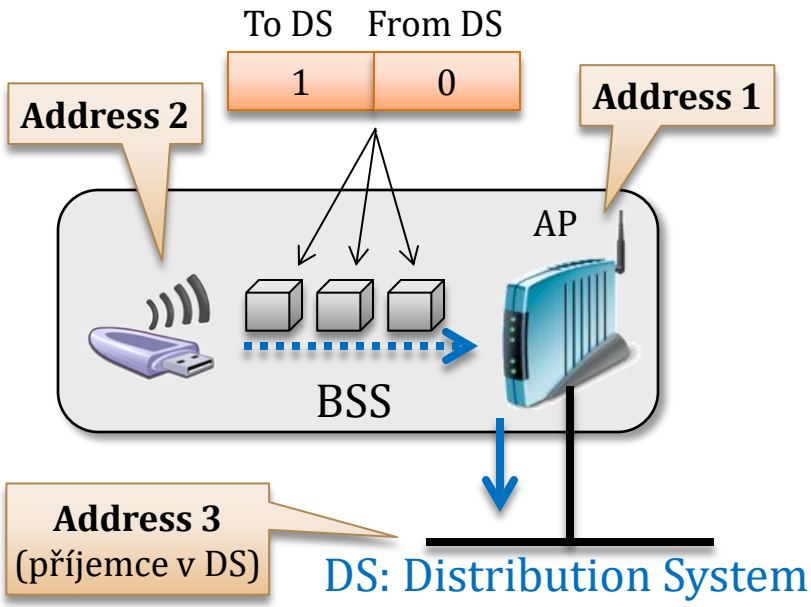
Type=01
- 1011: zpráva RTS (Request to Send), 1100: zpráva CTS (Clear to Send)
- 1101: zpráva ACK (potvrzení doručených dat)
- ……..

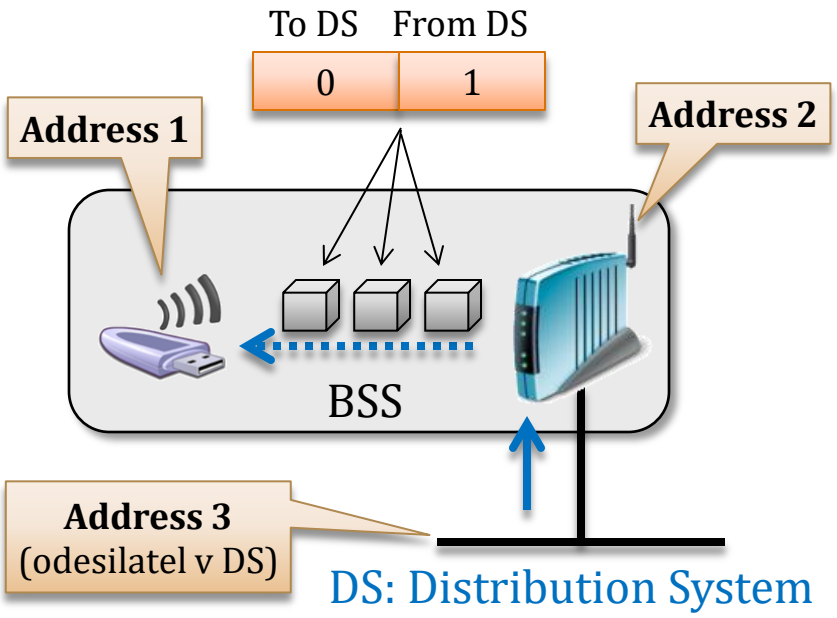
Type=10
- 0000: Data (datový rámec)
- 0100: Null Data (prázdný datový rámec, nenese žádná užitečná data)
- …….

formát MAC rámců 802.11

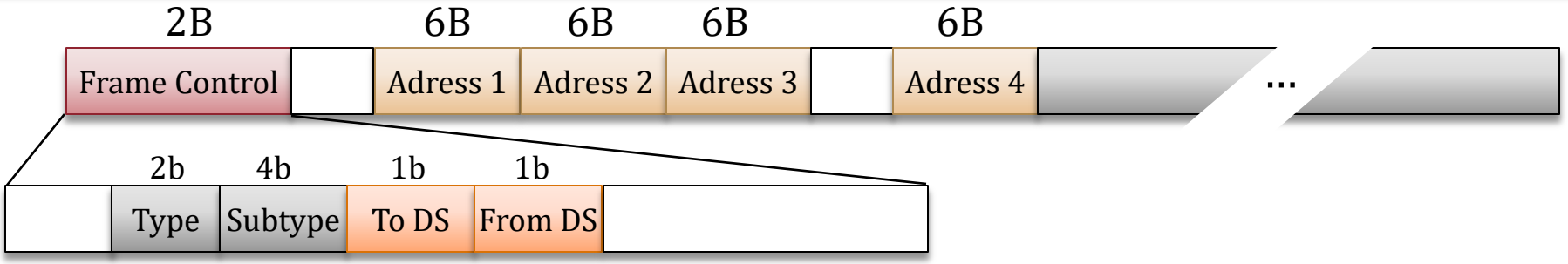


- **příznaky „To DS“ a „From DS“**
  - týkají se toho, zda (datový) MAC rámec směřuje z/do distribučního systému
    - a podle toho jsou nastaveny i MAC adresy v MAC rámci
      - musí rozlišit 3 adresy: STA, AP a uzlu v DS

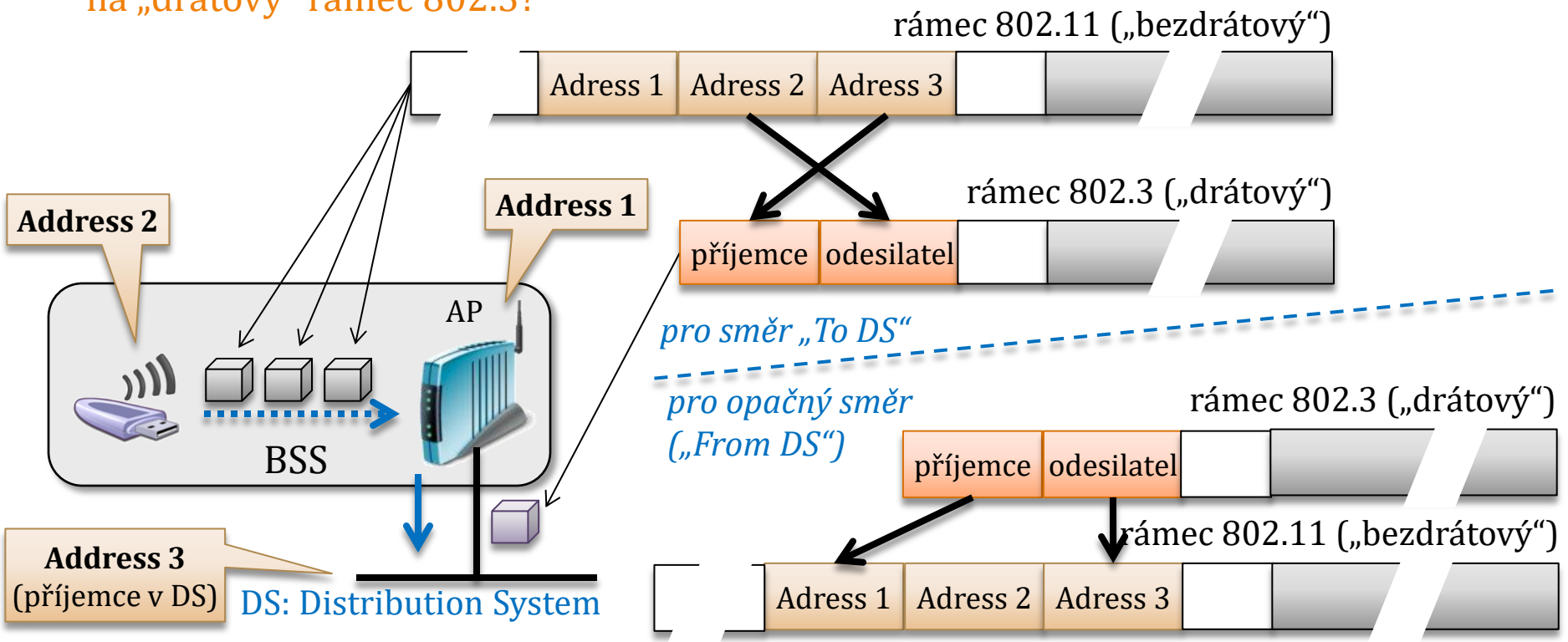




formát MAC rámců 802.11

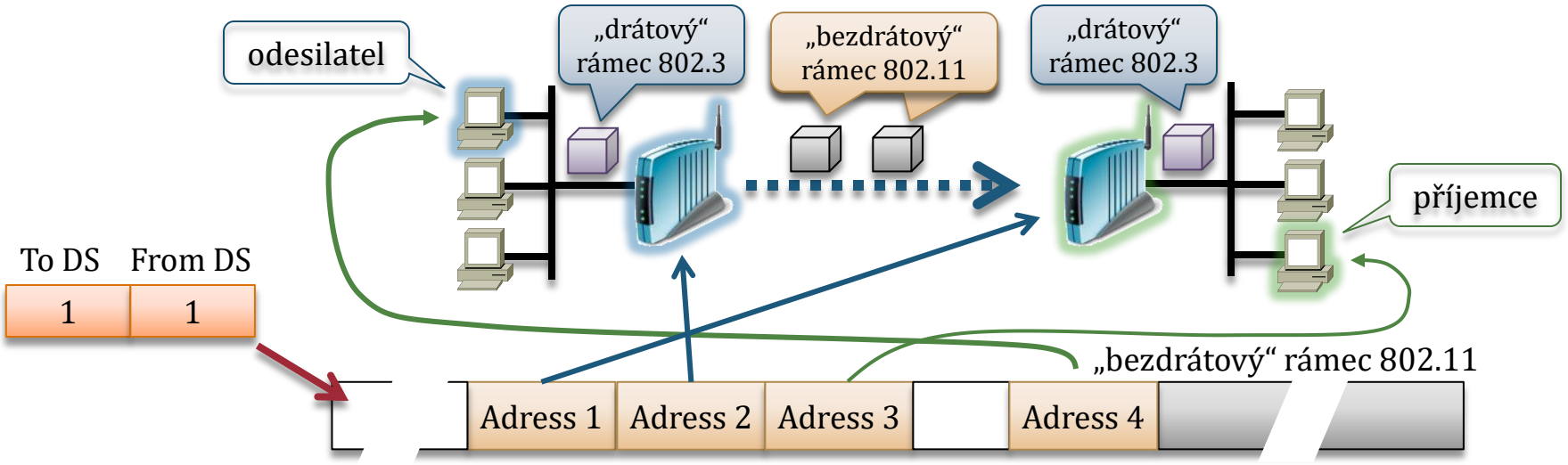


- **otázka (na fungování služby Integration):**
  - jak se překládají MAC adresy při převodu „bezdrátového“ datového MAC rámce 802.11 na „drátový“ rámec 802.3?

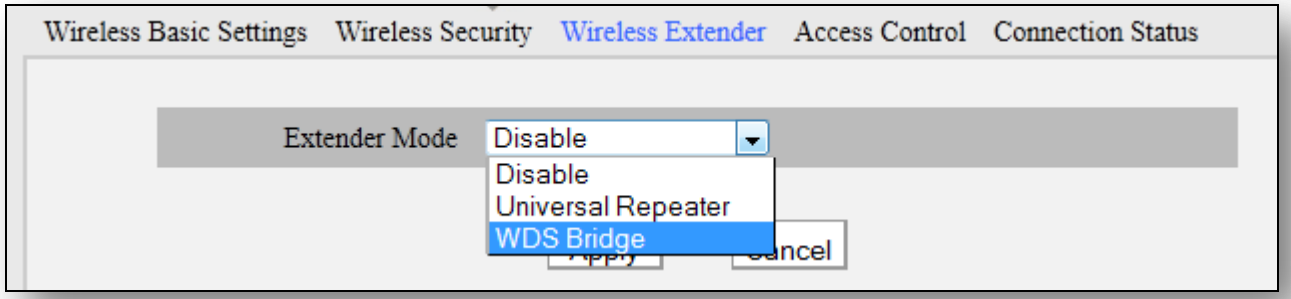


bezdrátový distribuční systém

- **odbočení:**
  - k čemu je v „bezdrátovém“ MAC rámci (rámci IEEE 802.11) 4. MAC adresa?
- **pro případ použití bezdrátového distribučního systému**
  - **WDS: Wireless Distribution System**, někdy též: **Wireless Bridge, WDS Bridge, ...**
  - jde o řešení pro bezdrátové propojení dvou drátových segmentů



  - přístupový bod (AP) ale musí umět pracovat v takovémto režimu
    - ne každý to umí



odbočení: režim ad-hoc

- **buňka bezdrátové sítě (BSS) nemusí fungovat jen dosud popisovaným způsobem**

  jsou součástí nějaké „větší síťové infrastruktury“

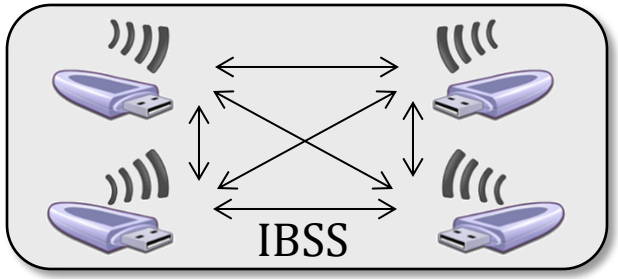
  - v režimu infrastruktury: s příst. bodem (AP) a napojením na distribuční systém (DS)
    - toto je obvyklé řešení – pro „plánované“ bezdrátové sítě
      - takové bezdrátové sítě, které si někdo dopředu vytvoří (např. doma, v kanceláři, škole, …), a pak je opakovaně používá
        - typicky: jejich přístupové body (AP) jsou umístěny pevně (nepřemisťují se), a jsou propojeny mezi sebou a napojeny na pevné (drátové) sítě pomocí distribučních systémů (DS)
- **alternativa:**
  - buňka (BSS) může fungovat **v režimu ad-hoc**, jako tzv. **Independent BSS (IBSS)**
    - nemá žádný přístupový bod

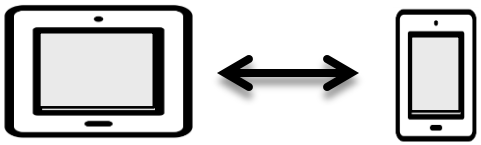
      

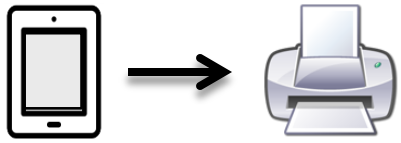
      - všechny uzly jsou si rovné („peers“)
        - a komunikují mezi sebou přímo
      - buňka je izolovaná od okolního světa
        - není napojena na žádný distribuční systém
        - proto pro všechny MAC rámce platí:

To DS	From DS
0	0

  - typické využití:
    - pro „spontánní“ propojení mobilních zařízení
      - za účelem jejich dočasné komunikace
        - např. přenos souborů mezi tablety, tisk na tiskárně apod.







řídící rámce a rámce pro správu

- **tyto MAC rámce (dle 802.11) „nepřechází“ do distribučního systému (DS)**
  - přenáší se jen mezi stanicemi (STA) a přístupovými body (AP)
    - případně jen mezi stanicemi (STA) v rámci buněk, fungujících v režimu ad-hod (IBSSS)
  - proto pro tyto rámce musí být nastaveno

To DS	From DS
0	0

- **řídící rámce slouží potřebám řízení přístupu**
  - pro zprávy RTS/CTS, pro potvrzen ACK atd.
- **rámce pro správu zajišťují „agendu fungování buňky“**
  - ve smyslu „domluvy“ mezi stanicemi (STA) a přístupovými body (AP)
    - mj. pro potřeby autentizace (deautentizace), asociace (reasociace, de-asociace) atd.
  - ale také v podobě:
    - rámců **Probe** („výzva“)
      - vysílá je (z vlastní iniciativy) stanice, jako Probe Request, a vyzývá tím přístupové body (či jiné stanice) k určité reakci
        - testuje jejich existenci a dostupnost
      - ostatní uzly na tyto rámce odpovídají
        - existují „odpovědní“ rámce: Probe Response
    - rámců **Beacon** („maják“)

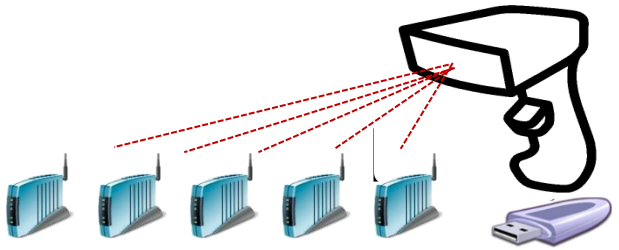
      - vysílá je (z vlastní iniciativy) přístupový bod, aby inzeroval svou existenci a své parametry

tento údaj lze skrýt (Hidden SSID)

        - například informoval o jméně sítě (SSID) a o dostupných možnostech přenosu
      - na tento druh rámců se neodpovídá
        - neexistuje rámec pro odpověď

skenování

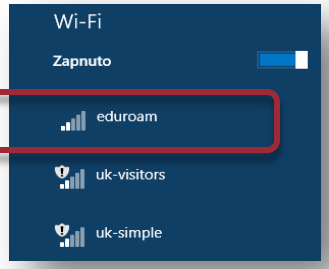
- **otázka:**
  - jak se konkrétní stanice (STA) dozví o tom, které sítě a buňky jsou v jejím dosahu?
    - včetně jejich parametrů: jmen sítí a buněk, podporovaných rychlostí, způsobů zabezpečení ....
- **možnosti:**

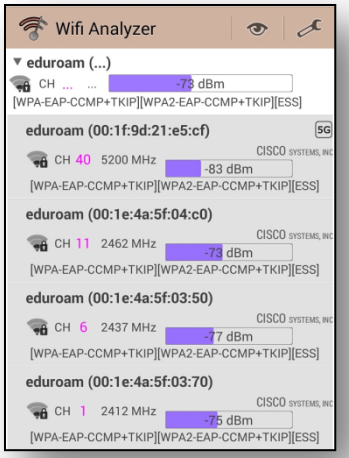


  - **aktivní skenování**
    - stanice (STA) sama vysílá výzvy (MAC rámce Probe Request) na konkrétních kanálech
      - musí to být frekvenční kanály, které je možné (povolené) využívat
        - viz licenční/bezlicenční pásma
    - tím sama vyzývá dostupné přístupové body, aby se ozvaly (formou rámců Probe Response)
      - v odpovědi přístupové body (AP) sdělují požadované informace o sobě
  - **pasivní skenování**
    - stanice (STA) pasivně poslouchá na zvoleném kanále
      - mohou to být i jiné než povolené kanály
    - čeká na rámce Probe Response nebo Beacon, z nich se dozví vše potřebné
- **k čemu (a jak) stanice využívá informace získané skenováním?**
  - pro výběr sítě (ESS) a přecházení mezi sítěmi („roaming“)
    - toto není součástí (základních) standardů IEEE 802.11 !!!!
      - řeší to uživatel, nebo aplikační SW na jeho stanici
  - pro výběr buňky (BSS) v rámci sítě (ESS) a přecházení mezi buňkami
    - toto je součástí standardů IEEE 802.11 a stanice by měly zajišťovat samy (automaticky)

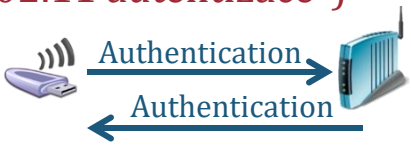
postup přihlašování k síti

- **jak se stanice (STA) dozví, ke kterému přístupovému bodu (AP) se má, resp. může asociovat?**
  - provede pasivní nebo aktivní skenování
    - aktivně: pomocí rámců Probe Request, pasivně čekáním na Beacon či Probe Response
    - dozví se o existenci sítí (získá jejich SSID) i jednotlivých přístupových bodů
      - i „sílu“ jejich signálu, požadavky na zabezpečení, i další parametry ….
  - svému uživateli může sestavit seznam dostupných sítí
    - i s příslušnými parametry
      - jméno sítě, zabezpečení, síla signálu





- **volbu sítě provede uživatel**
  - „ručně“ vybere síť
  - pokud je v takto zvolené síti více přístupových bodů (AP), stanice mezi nimi sama vybere ten, který je (podle ní) nejlépe dostupný
    - k takto zvolenému přístupovému bodu se stanice nejprve autentizuje („802.11 autentizace“)
      - stanice (STA) vyšle k přístupovému bodu MAC rámec Authentication
        - identitou stanice je její MAC adresa (48-bitová Ethernet adresa)
        - autentizačním údajem buď není nic (Open System Authentication), nebo WEP klíč
      - přístupový bod odpoví, opět pomocí MAC rámce Authentication

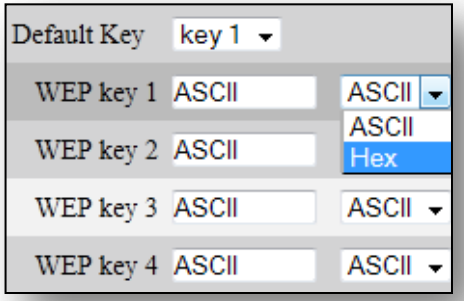


    - následně se stanice k přístupovému bodu asociuje
      - stanice pošle Association Request, přístupový bod odpoví pomocí Association Response

zabezpečení sítí dle 802.11

- **dosud popisované zabezpečení**
  - vychází ze standardů IEEE 802.11 z roku 1999 (IEEE 802.11-1999), zahrnuje
    1. autentizaci: jde o autentizaci stanice (nikoli uživatele), řeší se sdílením WEP klíče
    2. důvěrnost (šifrování) dat: řeší se pomocí algoritmu **WEP** (**Wired Equivalent Privacy**)
- **WEP používá šifru RC4 a původně pracoval s klíči o velikosti 64 bitů**
  - 40 bitů základu klíče (proto: WEP-40), 24 bitů inicializační vektor
    - bylo to dáno hlavně exportním omezením šifrovacích technologií ze strany USA
    - 40-bitové základy pro 64-bitové WEP klíče se zadávaly jako posloupnost 10 hexadecimálních čísel (0-9,A-F), tj. 10x4 bity, nebo jako 5 ASCII znaků (5x8 bitů)
- **později (bez exportních omezení) se používal WEP s klíčem 128 bitů**
  - 104 bitů základu klíče (WEP-104), 24 bitů inicializační vektor
    - 104-bitů základu se zadávalo jako 26 hexadecimálních čísel
- **toto zabezpečení se velmi brzy ukázalo jako příliš slabé!!!**
  - WEP-u lze zadat až 4 různé klíče, ale přepínat mezi nimi musí sám uživatel
    - WEP jinak pracuje stále se stejným klíčem
      - což významně usnadňuje prolomení WEP-u
        - při dostatečně dlouhém odposlechu

v roce 2004 Wi-Fi Alliance WEP oficiálně „pohřbila“



cca 2001/2002: bylo nezbytné postarat se o rychlou nápravu !!!

IEEE 802.11i

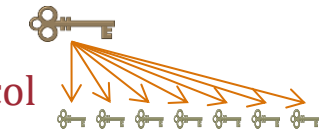
- **v roce 2004 byl přijat standard IEEE 802.11i (týkající se bezpečnosti)**
  - jako doplněk původního standardu IEE 802.11 (z roku 1999), který:
    - mění tu část původního standardu, která definovala oblasti autentizace a důvěrnosti (privacy)
      - hlavně: slabý a zranitelný WEP nahrazuje silnějšími metodami
        - a umožňuje autentizovat i konkrétní uživatele (a ne pouze stanice jako takové)
- **konkrétně:**
  - protokol TKIP nahrazuje protokolem **CCMP**
    - který vychází z **AES**
      - Advanced Encryption Standard
    - pro šifrování používá klíče velikosti 128 bitů a šifruje bloky o velikosti 128 bitů
      - „master key“, ze kterého CCMP odvozuje šifrovací klíče, má 256 bitů
    - zajišťuje:
      - šifrování přenášených dat
        - a tím jejich důvěrnost
      - ochranu proti jejich změně
        - tj. zajišťuje jejich integritu

Counter Cipher Mode with Block Chaining Message Authentication Code Protocol

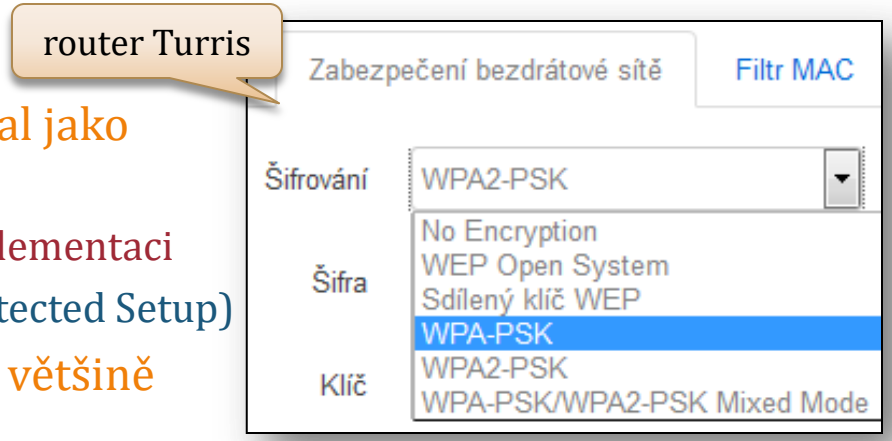
  - mění způsob autentizace
    - původně 2 možnosti:
      - Open System Authentication: žádná autentizace, každá stanice je autentizována
      - Shared Key Authentication: autentizace skrze znalost sdíleného WEP klíče
    - nově jiné 2 možnosti:
      - **Enterprise**: řešení vhodné pro firmy, umožňuje autentizovat konkrétní uživatele
      - **Personal** (též: **PSK**, Pre-Shared Key): jednodušší řešení, na bázi znalosti sdíleného klíče

WPA (Wi-Fi Protected Access)

- **jde o (dočasné) řešení, které vytvořila Wi-Fi Alliance v roce 2003**
  - není to standard IEEE 802.11
  - vychází z pracovní verze standardu IEEE 802.11i (ten byl dokončen až v roce 2004)
    - *„WPA vzniklo z nedočkavosti – práce na standardu nepokračovaly dostatečně rychle, a Wi-Fi Alliance se nemohla dočkat .... proto vydala nehotové řešení .... jako WPA .....„*
- **hlavní odlišnosti (oproti finální verzi standardu 802.11i):**
  - místo protokolu CCMP používá protokol **TKIP**
    - Temporal Key Integrity Protocol
      - z jednoho „výchozího“ klíče generuje dočasné šifrovací klíče, a rychle je střídá
        - aby se ztížila možnost odposlechu klíče, a tím možnost prolomení šifrování



  - pro zajištění integrity přenášených zpráv (rámců) používá algoritmus **Michael**
    - Michael Message Integrity Code
      - zkratkou MIC
    - nahrazuje CRC, používané u WEP-u
- **dnes je WPA překonané**
  - hlavně kvůli protokolu TKIP, který se ukázal jako slabý a zranitelný
    - ale také kvůli dalším „slabým místům“ v implementaci
      - například v rámci funkce WPS (Wi-Fi Protected Setup)
  - přesto je WPA dodnes implementováno ve většině Wi-Fi zařízení



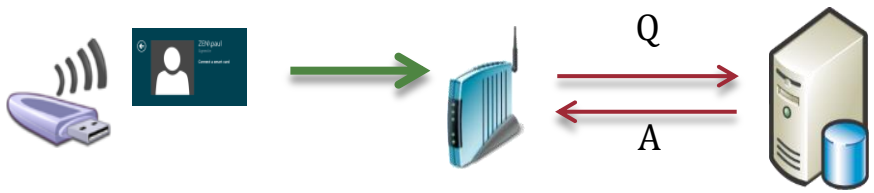
WPA 2 (Wi-Fi Protected Access 2)

- **WPA2 je „finálním“ řešením (z roku 2006)**
  - opírá se o (finální verzi) standardu IEEE 802.11i
    - formálně: nejde o standard, ale o celý „bezpečnostní rámec“
      - a také o trademark: obchodní značku/chráněnou známku
    - stejně jako u WPA: od Wi-Fi Alliance
      - konkrétní zařízení jsou certifikována na podporu WPA či WPA2

- **hlavní rozdíl (oproti WPA):**
  - protokol TKIP byl nahrazen „bytelnějším“ protokolem **CCMP**
    - tak, jak to požaduje (finální verze standardu 802.11i) protokol CCMP zajišťuje:
  - protokol CCMP zajišťuje
    - šifrování přenášených dat, a tím jejich důvěrnost (u WPA toto zajišťoval protokol TKIP)
    - ochranu přenášených dat proti změně, resp. zajištění integrity (toto u WPA dělal Michael MIC)
- **existuje i tzv. smíšený režim (WPA/WPA2 mixed mode)**
  - týká se přístupových bodů (AP)
    - umožňuje, aby v jedné buňce (BSS) koexistovaly stanice fungující dle WPA i stanice WPA2
  - princip fungování smíšeného režimu:
    - přístupový bod „inzeruje“ (ve svých beacon rámcích), jaké šifrování podporuje
      - TKIP, CCMP či jiné
    - stanice, která se chce asociovat, si vybere šifrování, které pak vůči přístupovému bodu používá

autentizace dle IEEE 802.11i

- **původní standard (IEEE 802.11-1999):**
  - řešil autentizaci (z dnešního pohledu) nedostatečně, „slabě“ a nevhodně
    - autentizovala se pouze stanice
      - identifikovala se pomocí své MAC adresy, autentizovala nijak / pomocí sdíleného WEP klíče
        - všechny stanice se autentizovaly stejně (pomocí stejných WEP klíčů)
    - nedal se brát zřetel na to, kdo je uživatelem stanice
    - WEP byl příliš slabý a zranitelný (navíc se používal současně i pro šifrování)
    - ani samotný postup autentizace (přenos autent. údajů, komunikace obou stran) nebyl ideální
- **nový standard (IEEE 802.11i-2004) mění celou koncepci autentizace**
  - zavádí dva různé režimy autentizace
    - **WPA(2) Enterprise** (pro firmy, …)
      - identifikuje a autentizuje se uživatel
        - uživatel poskytne přístupovému bodu (AP) své autentizační údaje, a přístupový bod si podle nich ověří identitu stanice u autentizačního serveru
          - např. u serveru Kerberos, …..

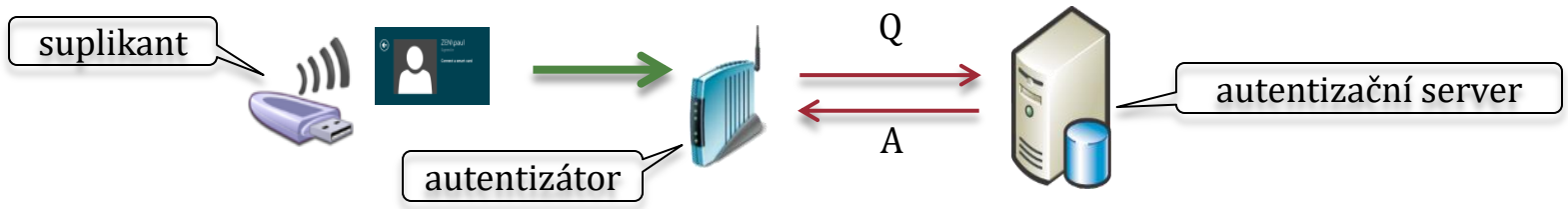


princip fungování je stejný jako původně (u 802.11-1999)

- **WPA(2) PSK,** též: **WPA(2) Personal**
  - vhodné pro domácnosti, ….
  - identifikuje a autentizuje se stanice
    - všechny stanice (STA) se vůči přístupovému bodu (AP) prokazují znalostí stejného (předem na-) sdíleného klíče
      - **PSK: Pre-Shared Key**
      - není nutný žádný autentizační server

IEEE 802.1x

- **jde o samostatný standard od IEEE (pracovní skupiny 802.1)**
  - umožňuje autentizaci zařízení, která se chtějí „přihlásit“ do (drátových) sítí LAN, či do (bezdrátových) sítí WLAN
    - dokáže brát ohled na konkrétní uživatele
      - použité identifikační a autentizační údaje mohou patřit uživateli (a ne stanici jako takové)
    - dokáže soustředit (lokalizovat) „rozhodování“ do jednoho místa
      - posuzování a hodnocení identifikačních a autentizačních údajů (tzv. credentials) zajišťuje jeden společný server
        - jeden autentizační server, společný pro více přístupových bodů (AP)
          - ke kterým se stanice (STA) se svými uživateli přihlašují
  - je nezávislý na konkrétních způsobech a metodách identifikace a autentizace
    - neříká, jaké konkrétní údaje mají sloužit pro identifikaci a autentizaci (ani koho .....)
      - ani jak mají být vyhodnocovány a posuzovány
  - terminologie:
    - **suplikant**: „*ten, kdo žádá o přístup / přihlašuje se*“ (stanice, resp. SW běžící na stanici)
    - **autentizátor**: „*ten, kdo přiděluje přístup ....*“ (přístupový uzel / AP)
    - **autentizační server**: „*ten, kdo o přístupu rozhoduje*“ (společný autentizační server)

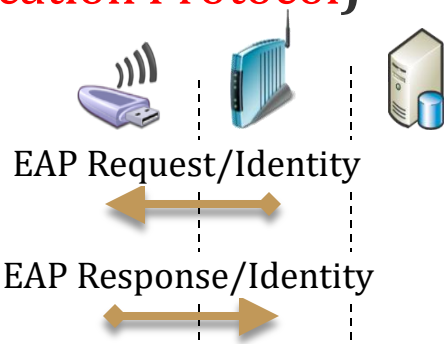


EAP (Extensible Authentication Protocol)

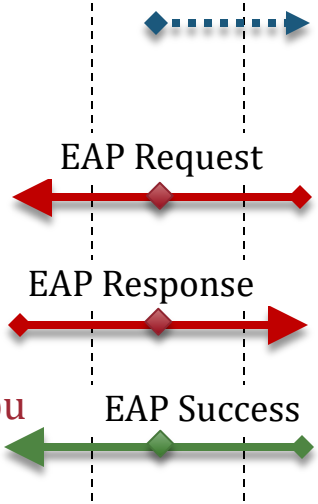
- **standard IEEE 802.1x předpokládá, že:**
  - existuje mechanismus (protokol) pro vzájemnou komunikaci mezi všemi 3 prvky
    - mezi suplikantem, autentizátorem a autentizačním serverem
      - aby si mohli vzájemně předávat požadované údaje, žádosti i odpovědi
- **takovým protokolem je protokol EAP (Extensible Authentication Protocol)**
  - příklad dialogu:

volitelně

- autentizátor (AP) vyzve suplikanta (STA), aby se identifikoval
  - pošle mu žádost EAP-Request/Identity
- suplikant (STA) pošle autentizátorovi (AP) své identifikační údaje
  - pošle mu odpověď EAP-Response/Identity

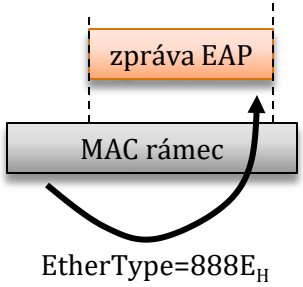


- autentizátor (AP) se obrátí na autentizační server
  - pokud neodmítne žadatele (suplikanta) již na základě jeho identity
- autentizační server pošle suplikantovi žádost o poskytnutí autentizačních údajů
  - zprávu EAP-Request, posílá ji zprostředkovaně přes autentizátora (AP)
- suplikant (STA) poskytne autentizačnímu serveru své autentizační údaje
  - zprávu EAP-Response, posílá ji zprostředkovaně přes autentizátora (AP)
- autentizační server posoudí poskytnuté údaje a rozhodne o povolení přístupu
  - vrátí zprávu EAP-Success (nebo EAP-Failure)
    - autentizátor ji předá suplikantovi, sám na jejím základě povolí/nepovolí přístup

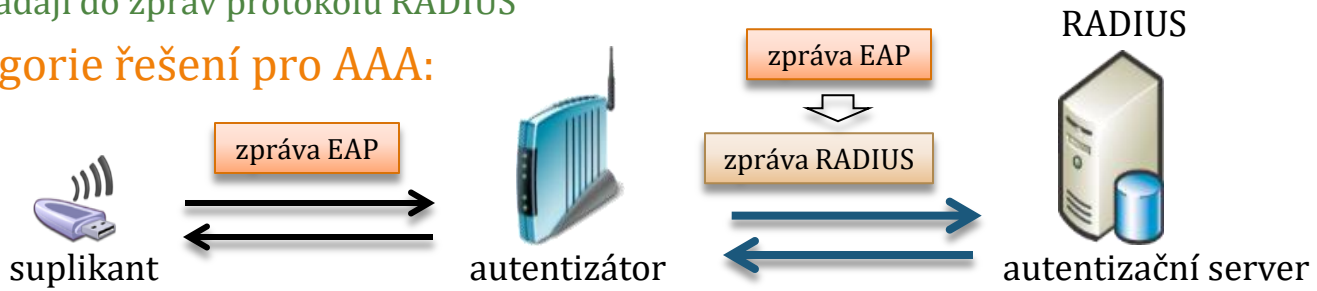


EAP, EAPOL, RADIUS a IEEE 802.1x

- **EAP je obecné řešení, původně vyvinuté pro protokol PPP**
  - umožňuje i „opačný směr“ autentizace: aby stanice (STA) věděla, k čemu se přihlašuje
    - aby se jí identifikoval a autentizoval přístupový bod (AP / Autentizátor)
      - a stanice (resp. její uživatel) věděli, komu poskytují své identifikační a autentizační údaje
- **EAPOL (EAP over LAN) je konkrétní variantou EAP**
  - určenou pro nasazení a fungování v prostředí sítí LAN (nad Ethernetem či Wi-Fi)
    - zprávy EAP se vkládají do ethernetových linkových rámců
      - u „drátových“ sítí Ethernet s EtherType=$888E_H$
- **standard IEEE 802.1x používá právě EAPOL**
  - resp. **EAPoW** (EAP over Wireless), pro vkládání do MAC rámců 802.11



- **RADIUS (Remote Authentication Dial In User Service)**
  - je obvyklým řešením pro autentizační server (v rámci IEEE 802.1x)
    - má vlastní protokol pro komunikaci se svými klienty zpráva RADIUS
      - zde: pro komunikaci autentizačního serveru s autentizátorem (AP)
        - zprávy EAP se vkládají do zpráv protokolu RADIUS
  - RADIUS spadá do kategorie řešení pro AAA:
    - Authorization
    - Authentication
    - Accounting



rozšíření EAP

- **EAP je pouze obecným rámcem pro autentizaci**
  - nedefinuje konkrétní metody a postupy autentizace
    - ty definují až jeho rozšíření (proto také: „Extensible“ Authentication Protocol)
  - rozšíření protokolu EAP se týkají:
    - celkové metody
      - řeší hlavně způsob přenosu údajů suplikantem a autentizačním serverem
      - EAP-TLS
        - vzniká zašifrované spojení, na bázi TLS
          - je nutný SSL certifikát autentizačního serveru
          - je nutný SSL certifikát suplikanta
      - EAP-TTLS
        - jako EAP-TLS, ale stačí jen certifikát serveru
      - PEAP: Protected EAP
        - jako EAP-TTLS, ale s podporou Microsoft-u
      - EAP-SIM, EAP-AKA
        - využívají se SIM karty (USIM karty v UMTS)
      - ……
    - konkrétního postupu/procesu ověření
      - PAP (Password Authentication Protocol)
        - jméno a heslo, bez dalšího zabezpečení
          - 2-fázový handshake
          - použitelné jen v rámci TTLS
      - CHAP (Challenge Handshake Authentication Protocol)
        - bezpečnější než PAP
          - 3-fázový handshake
          - použitelné jen v rámci TTLS
      - MS-CHAP-V2
        - varianta CHAP
          - pochází od Microsoft-u
      - GTC (Generic Token Card)
        - možnost využití tokenů a čipových karet

aut. server se prokazuje SSL certifikátem, klient (suplikant) mu musí důvěřovat

uživatel zadává své jméno a heslo

- **příklady:**
  - Eduroam používá: 802.1x s RADIUS, metodu PEAP a ověřování MS-CHAP-V2

příklad: přístup k síti Eduroam