# WIFI - bezpečnost

Wi-fi, WiFi, Wifi, wi-fi, wifi - slovní hříčka wireless fidelity

# Zabezpečení WLAN sítí

- Nezabezpečená bezdrátová síť WLAN:
  - nebezpečná hned z několika pohledů:
  - do nezabezpečené sítě – pronikne kdokoliv
  - mohou přistupovat ke všem sdíleným souborům
  - mohou se dostat i k datům na pevném disku

# Zabezpečení WLAN sítí

- Nezabezpečená bezdrátová síť WLAN:
  - kdokoliv cizí se může dostat přes vaše připojení do internetu:
    - A to pod vaším jménem (IP adresou)
- Vaším jménem lze konat trestnou činnost:
  - Provádět průniky/útoky do cizích sítí
    - (banky, armáda, státní orgány, firmy…)
  - zveřejňovat nelegální obsah
    - Porušování autorských práv, dětská pornografie
    - A řadu dalších a dalších trestných činností (phishing…)

# Zabezpečení WLAN sítí

- Orgány trestního řízení:
  - Díky IP adrese zjistí poskytovatele INETu
  - Následně jméno, příjmení a adresu majitele připojení (Vás)
    - vy se budete zodpovídat za porušení zákona
    - a vaše zařízení bude zabaveno
    - a při nejhorším – stanete se spolupachateli

# Zabezpečení WiFi sítí

- ZÁKLADNÍ METODY ZABEZPEČENÍ WI-FI
  1) Vhodný návrh umístění AP
     - Zamezení vysílání mimo perimetr (okolí vysílače)
  2) Vlastní zabezpečení sítě
     - Skládá se z několika postupných kroků
       - Čím více použitých metod – tím více překážek proti „prolomení“ sítě

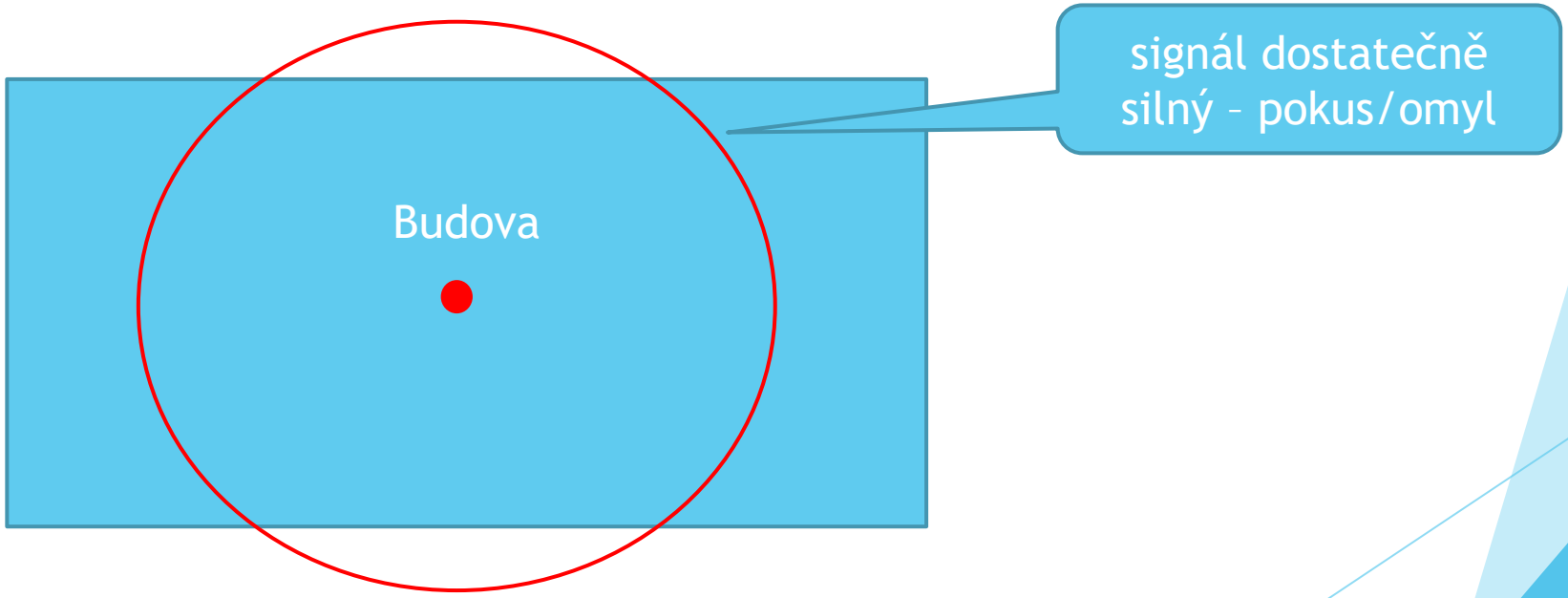
# Zabezpečení WiFi sítí

add 1) **Návrh bezpečné sítě**

- **Vhodné umístění AP** uvnitř budovy:
  - Podmínka - co nejlepší pokrytí signálem
  - Tak aby zbytečně nezasahoval mimo požadovaný prostor
- **Snížit vysílací výkon** (pokud to AP umožňuje)
  - Dostatečný výkon pro obsloužení všech stanic v oblasti
  - Snížený výkon – menší dosah „mimo“ požadovaný prostor
- **Použít sektorové antény**
  - budou mířit optimálně dovnitř požadovaného prostoru

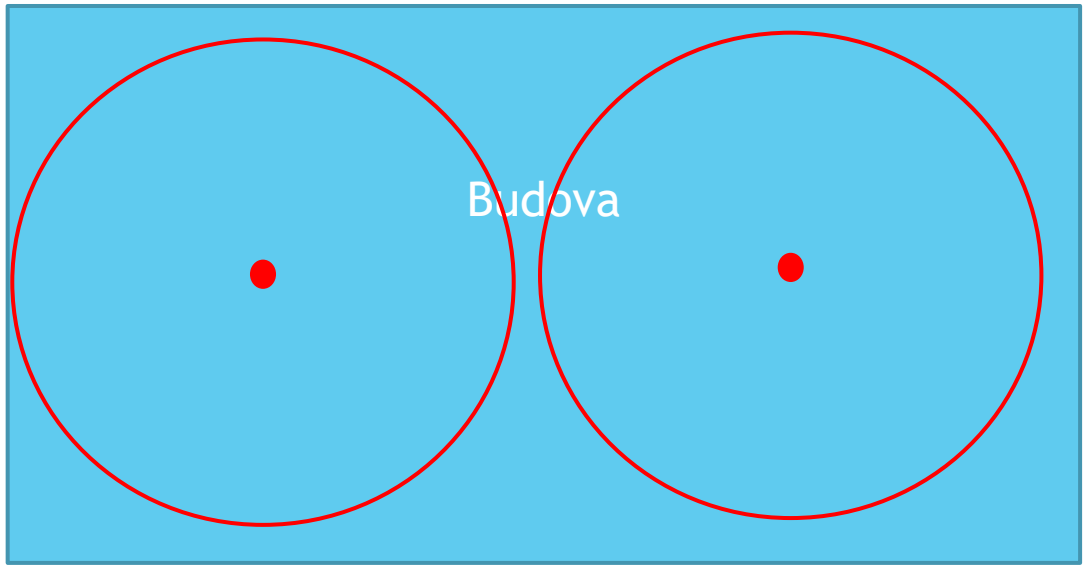
# Zabezpečení WiFi sítí

- Všesměrové vysílání – rozumné snížení výkonu antény:



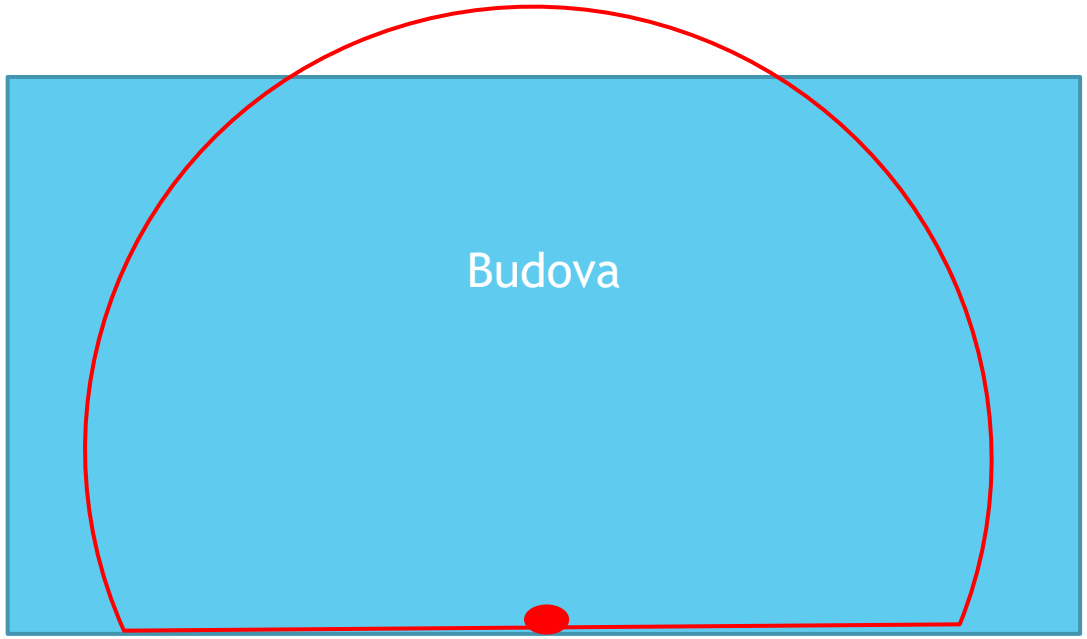
# Zabezpečení WiFi sítí

- Všesměrové vysílání – řešení více wifi zařízeními:
  - Např. Router – samostatné AP/ wifi repeator



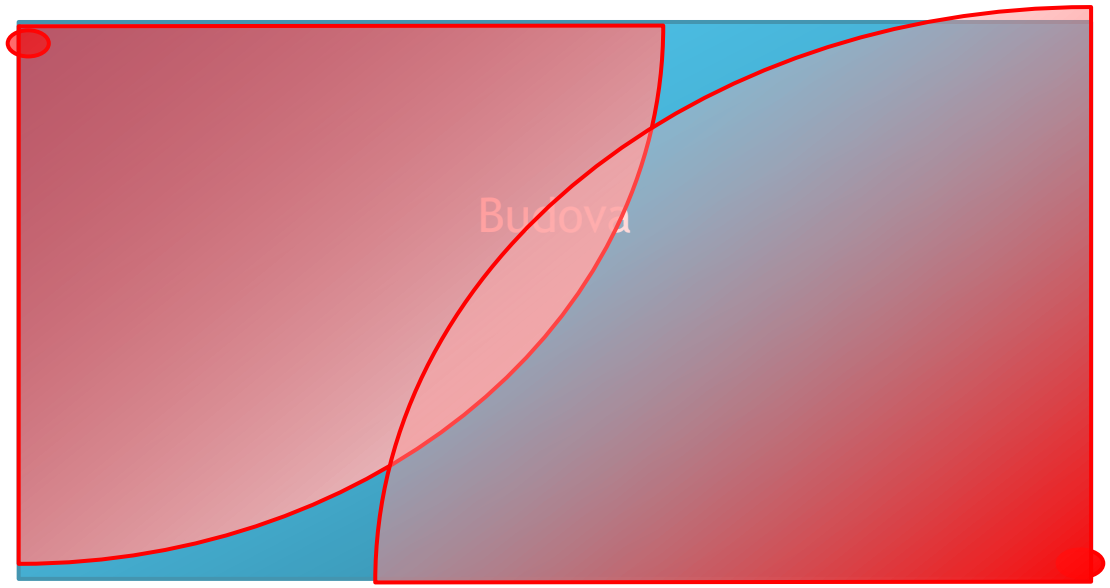
# Zabezpečení WiFi sítí

- Sektorové vysílání – asi nejlepší řešení:



# Zabezpečení WiFi sítí

- Sektorové vysílání – asi nejlepší řešení:



# add 2) Základní metody zabezpečení sítě

**Krok 1):** Změna defaultního **loginu a hesla** k nastavení AP:

- Známé hodnoty – tabulka na internetu/ údaje v manuálech zařízení
  - narušitel zná-li přístup - převezme kontrolu celé WLAN
- **Silné heslo:**
  - 10 a více náhodných znaků (neslovníkové)
  - ;+@#$%^&*()_{}… Aa…0..9
- **Nebo nesmysl proložený mezerami:**
  - Zd1vocela kroketa.na strome

# Zabezpečení WiFi sítí

**Krok 2:** Skrytí SSID

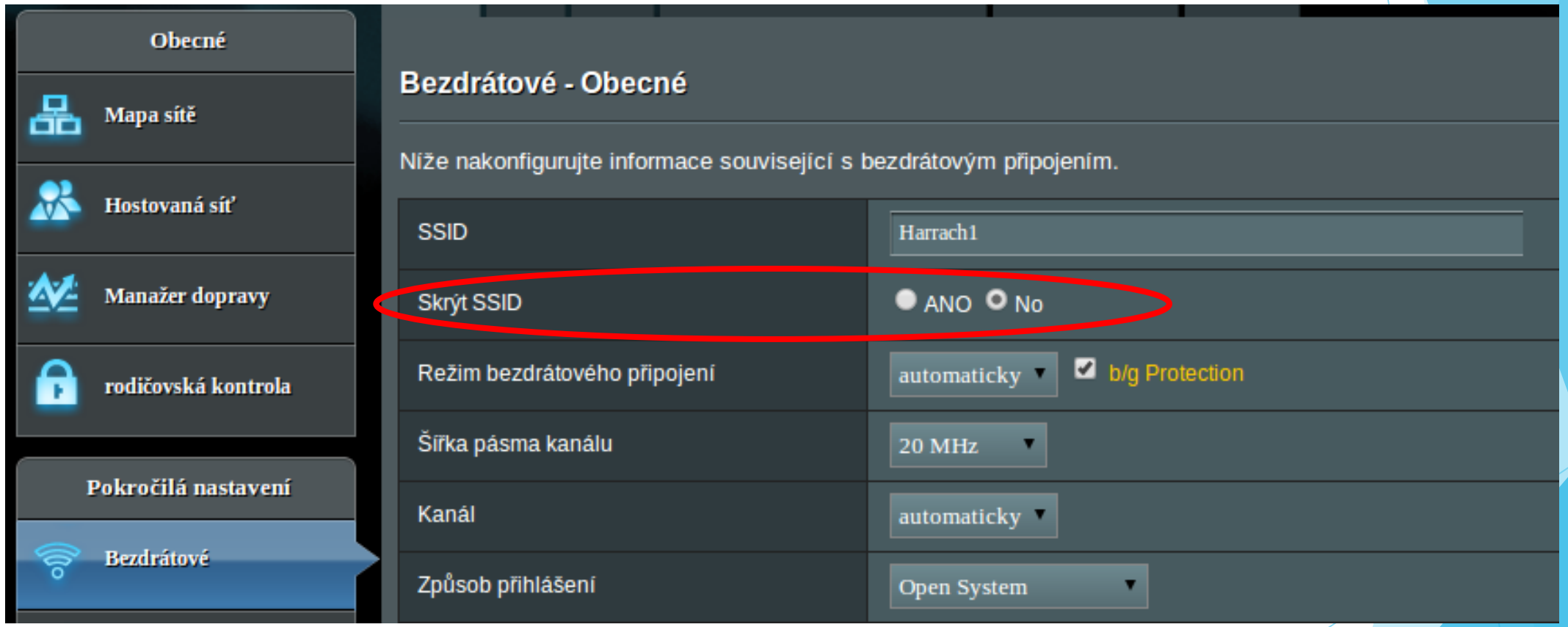
- **SSID -** údaj nezbytný k připojení do WiFi sítě
  - vhodnější SSID vůbec nevysílat – zakázat
  - některá AP neumožňují
- SSID - vždy přenášena v nešifrované podobě
  - Skryté SSID lze zjistit z komunikace mezi AP a klienty
  - odposlechem - monitorováním síťového provozu
- **Omezená účinnost:**
  - AP s klienty komunikuje přes BBSID (MAC adresy)

# Zabezpečení WiFi sítí

## Krok 2: Skrytí SSID

- Není bezpečné používat pouze tento typ ochrany
  - Použijeme-li „prázdý“ řetězec SSID:
    - lze se připojit k AP přes BSSID (MAC adresa AP)
      - ***B**asic **S**ervice **S**et **ID**entifier*
    - BSSID obsahuje každý datagram vždy a „neskrytě“

# Zabezpečení WiFi sítí



# Zabezpečení WiFi sítí

**Krok 3:** Vypnout službu DHCP

- Zakázat automatické přiřazení IP adresy klientům
- Klient musí znát IP adresu sítě:
  - svoji přidělenou IP adresu,
  - masku subnetu
  - Bránu
  - Volné IP Adresy – ošetřit ve firewallu routeru

# Zabezpečení WiFi sítí

## Krok 4: MAC adresy klientů

- Zapnout filtrování MAC adres
  - Evidence MAC adresy klientů v AP
- Samotný krok 4 - nedostatečná ochrana
- Lepší řešení:
  - MAC adrese lze přiřadit konkrétní IP adresu klienta
  - některé AP umožňují jen v režimu DHCP

# Zabezpečení WiFi sítí

Nejdůležitější krok 5: **Šifrované přihlášení a přenos dat**

1) WEP (starší zařízení) *Wired Equivalent Privacy*
   - Nedostatečné – šifrování prolomeno v 2001
     - Prolomitelné v minutách i chytrým telefonem
     - Používá se už jen u starších zařízení b/g
   - Používá tajný klíč pro šifrování dat
     - Obě strany při vzájemné komunikaci musí tento klíč znát.

# Zabezpečení WiFi sítí

## Šifrované přihlášení a přenos dat

2) WPA - *Wi-Fi Protected Access*

- Stejné šifrování jako WEP ale delší šifrovací klíč 128 bitový
  - Nedostatečné ale mnohem lepší než WEP
  - Slabé místo – správa klíčů TKIP
- WPA – TKIP (bezpečné asi jako WEP)
- WPA – PSK (lepší bezpečnost)
  - režim s předsdíleným heslem (Pre-shared key)
  - Sdílené heslo – nastaveno na všech AP a u klientů

# Zabezpečení WiFi sítí

## Šifrované přihlášení a přenos dat

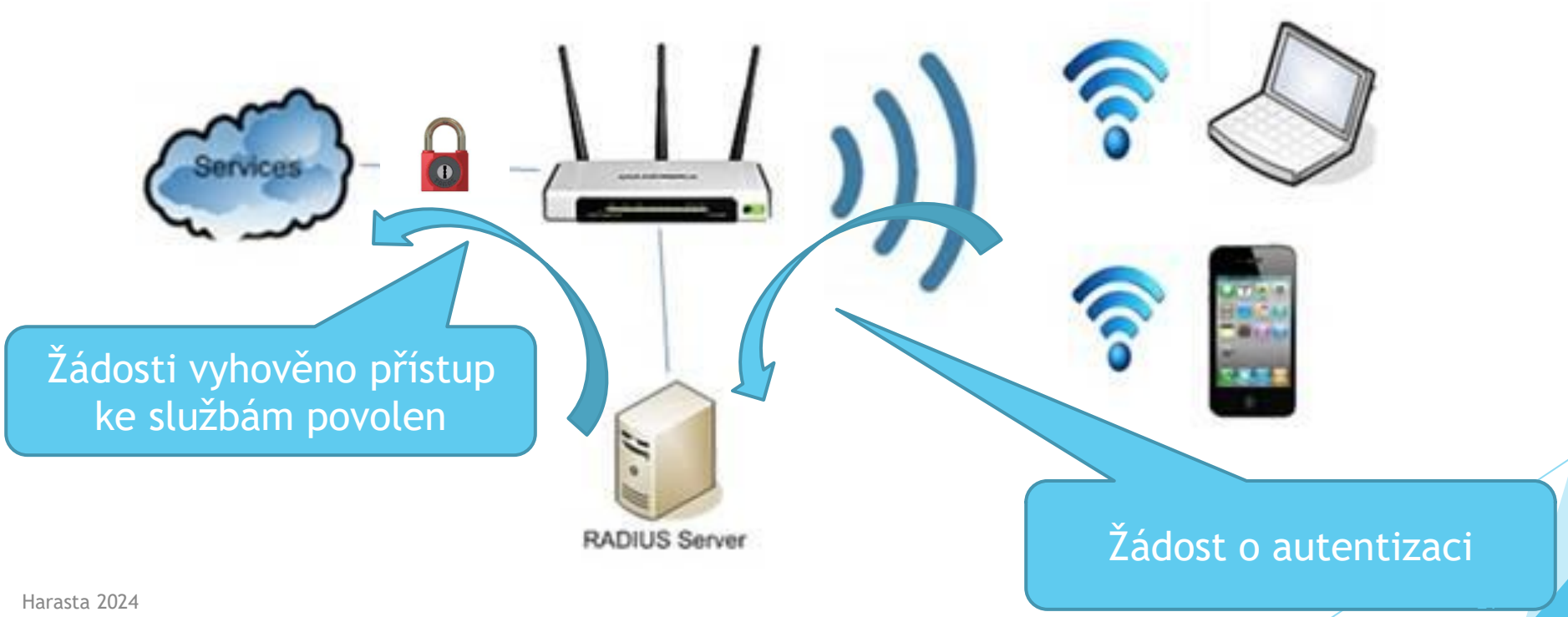
3) WPA2/WPA3 - šifrovací algoritmus AES (802.11i)
   - *Advanced Encryption Standard*
   - považován za zcela bezpečný, záleží už jen na kvalitě hesla
- Správa klíčů - protokoly rozšířeny a založeny na AES
  - Vždy vybírat varianty založené na AES !!!
- WPA2(TKIP/CCMP)/WPA3(GCMP) – personal (jedno spol.heslo)
- WPA2/WPA3 – enterprise:
  - firemní řešení s rozšířenou autentizací
  - ověření identity klienta – vysoká síťová bezpečnost

# Zabezpečení WiFi sítí

- Jak funguje **WPA2/WPA3 - enterprise**
  - Každý klient má svůj jedinečný login/heslo (tzv. autentizaci)
  - AP odešle požadavek přístupu klienta na RADIUS server (AAA)
    - RADIUS server (AAA) eviduje jedinečné loginy a hesla klientů
    - Server přístup do sítě potvrdí nebo zamítne
    - AP data pošle nebo zahodí
  - AAA – protokol:
    - *Authentication, Authorization and Accounting*
    - Vysoká bezpečnost – loginy/hesla a data zasílána šifrovaně

# Zabezpečení WiFi sítí

- Jak funguje **WPA2**/WPA3 **- enterprise** (AAA – RADIUS server)



# Zabezpečení WiFi sítí

## Šifrované přihlášení – kompatibilita zařízení

Připojení starších zařízení - WEP *k AP s WPA2/3*

- Nikdy nenastavovat **AP na WEP !!!**
- Lepší varianta:
  - Externí WiFi USB dongle s 802.11i (WPA2/**3**)
  - Cca od 200,- Kč a výše (802.11 /ax)…
  - Upřednostit WPA3