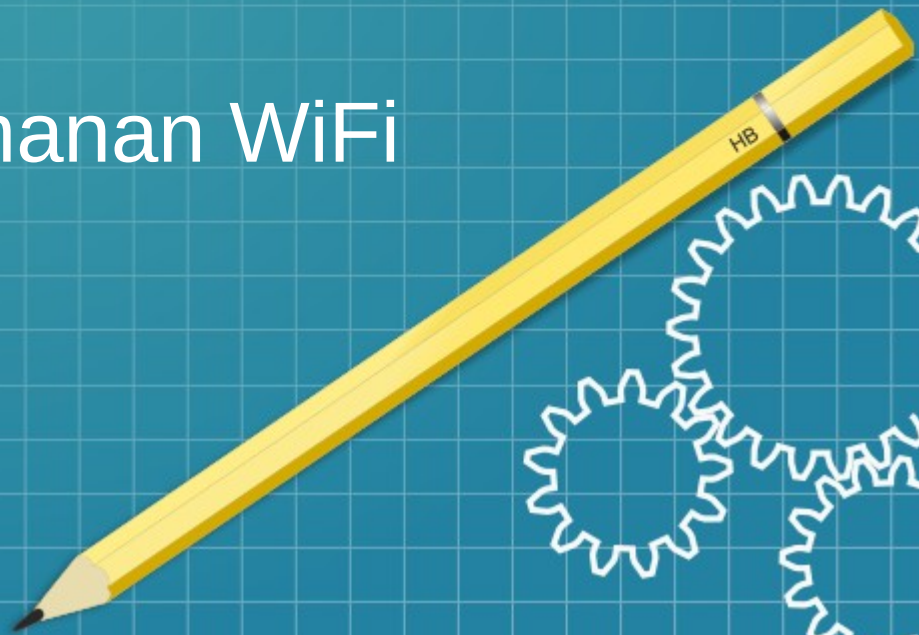
TIS13534P KOMUNIKASI DAN KEAMANAN DATA

Minggu 14 - Keamanan WiFi



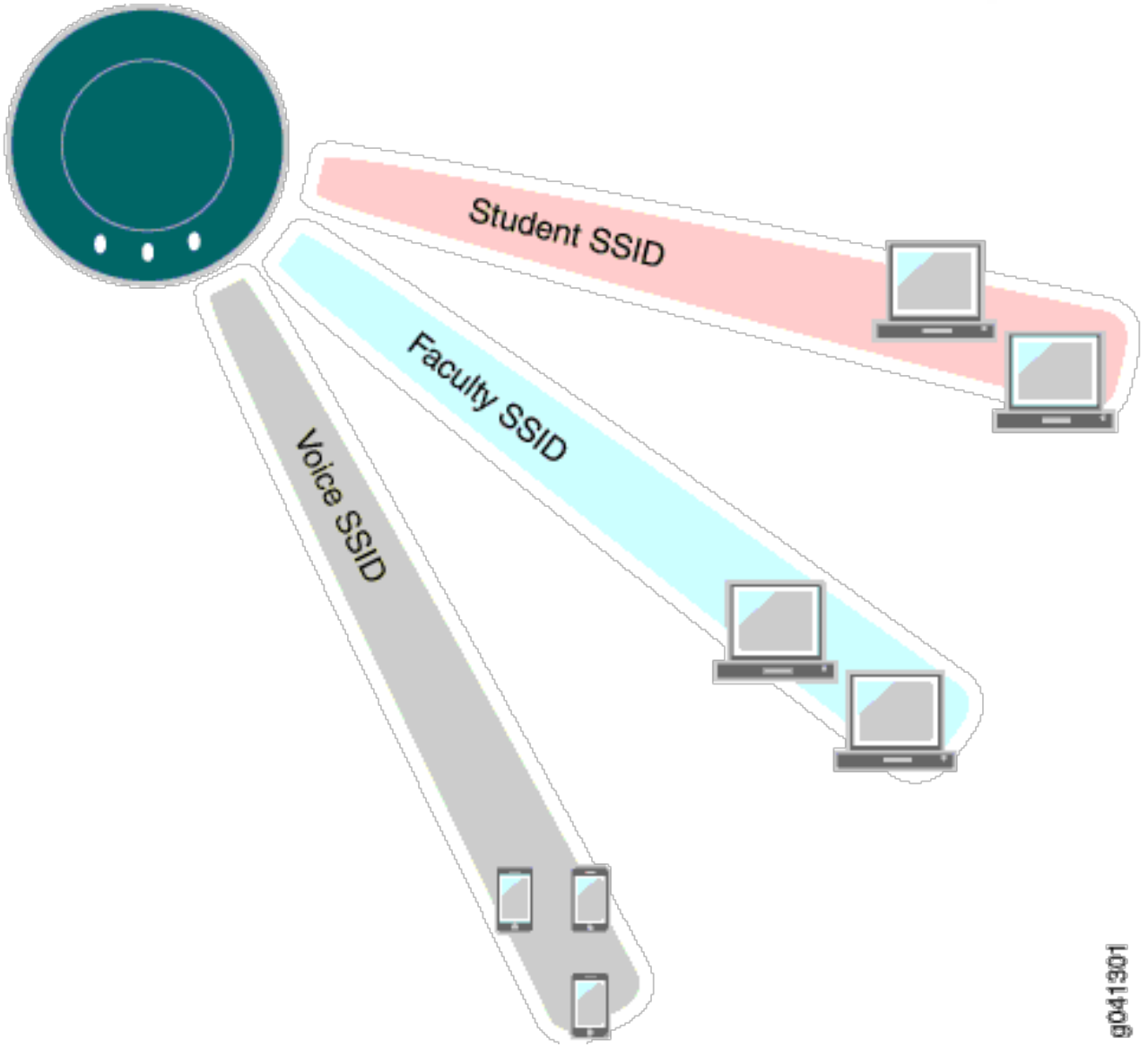
Apa Itu WiFi?

- Media untuk terkoneksi dengan jaringan tanpa menggunakan kabel
- Koneksi ini mengandalkan gelombang radio dengan frekuensi 2.4GHz atau 5GHz
- Sehingga dalam penggunaannya tidak mengganggu perangkat lain seperti telepon genggam, radio, televisi analog.
- Komunikasi yang digunakan pun dua arah.

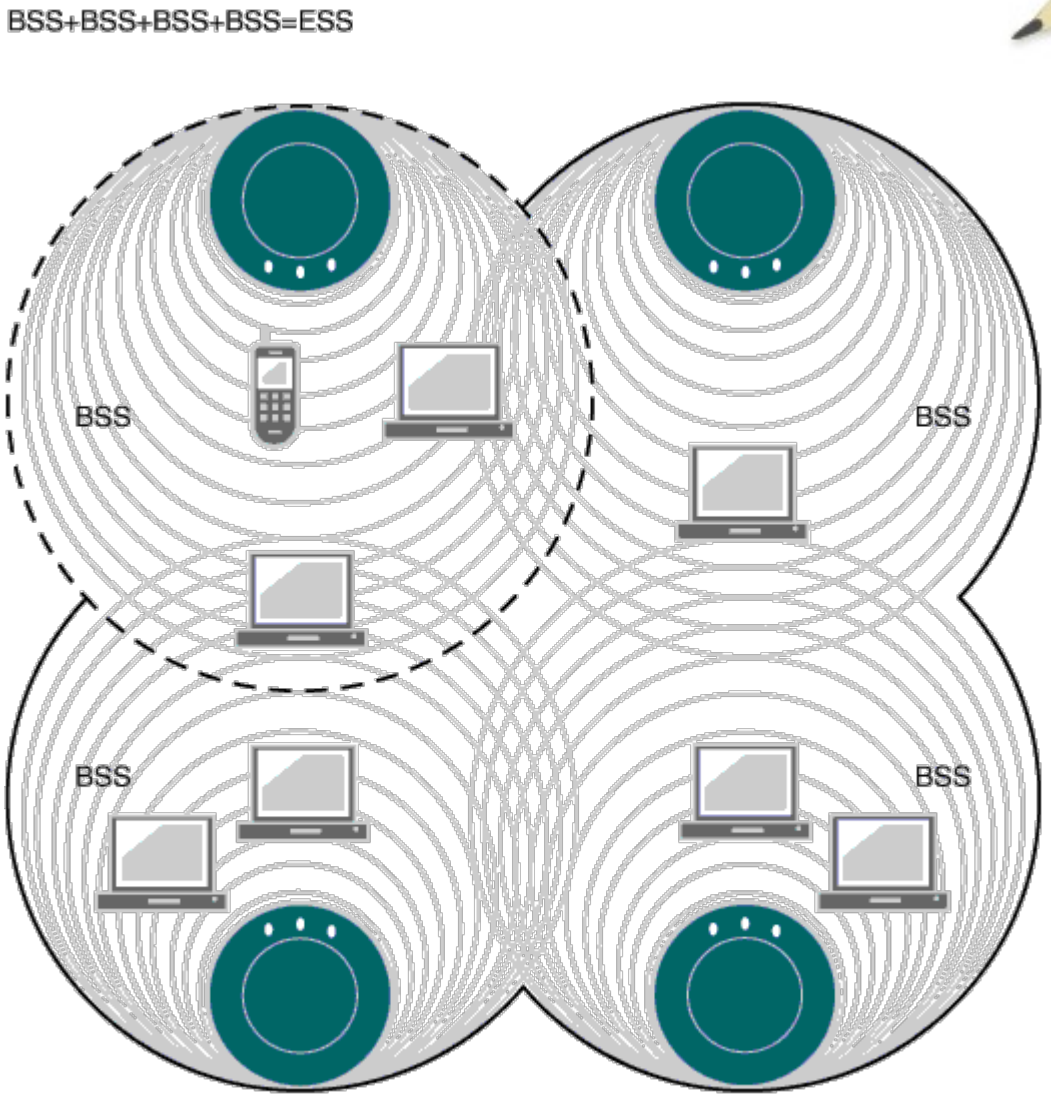
Istilah-Istilah WIFI

- Service Set ID (SSID): Nama yang bisa dilihat ketika akan melakukan koneksi WIFI
- Basic Service Set ID: Identifikasi Akses Point dan Kliennya
  - Independent Basic Service Set untuk Ad Hoc
- Extended Service Set ID: Kumpulan dari beberapa BSS

Ilustrasi SSID



Ilustrasi BSSID



Perbandingan

	Kabel	**Wireless**
Jumlah Host	1 Kabel 1 Host	1 Hotspot Banyak Host
Jangkauan	100m untuk CAT-5e	Tergantung Lingkungan
Mobilitas	Tergantung letak kabel	Bisa berpindah-pindah selama ada di dalam jangkauan
Keamanan	Aman	Banyak Penguping

Mode Jaringan Wireless

- Peer-to-Peer / Mode Ad Hoc
- Client-Server / Mode Access-Point (Hotspot)

Peer-to-Peer

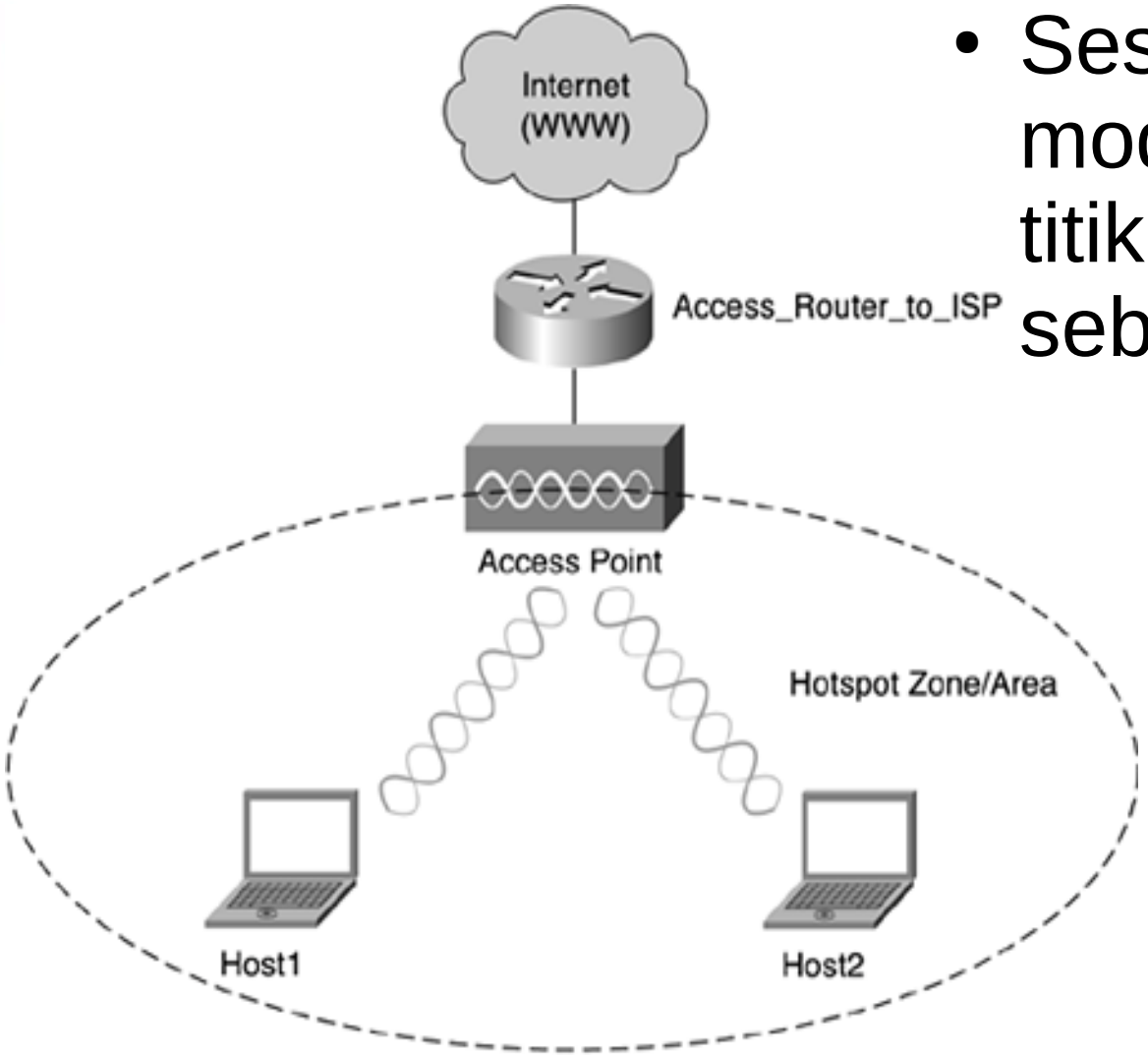
- Setiap Node atau perangkat yang ada di jaringan ini tidak ada yang memegang peran sebagai server.
- Semua terkoneksi melalui topologi Mesh, yang di mana semua komputer terhubung satu sama lain secara logika
- Jika satu peer down, maka peer lain tetap aktif

Ilustrasi

Peer-to-Peer / Ad-Hoc

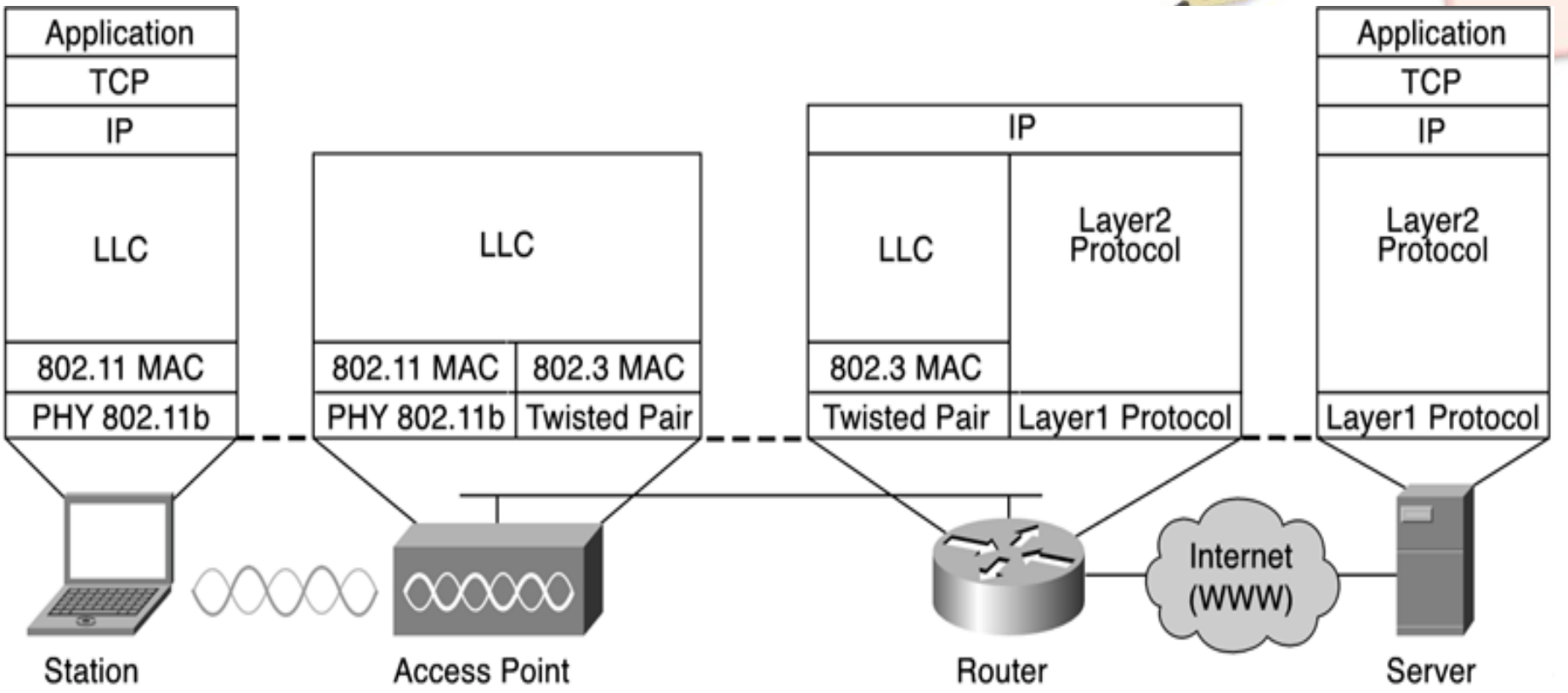
- Untuk mengaktifkan mode Ad-Hoc diperlukan konfigurasi khusus di salah satu komputer saja. Komputer lain hanya tinggal konek saja

Mode Access Point



- Sesuai namanya, mode ini memerlukan titik akses pusat sebagai penyedia

Cara Kerja WIFI



- Cara kerja WIFI berbeda dengan Kabel, standar WIFI adalah 802.11

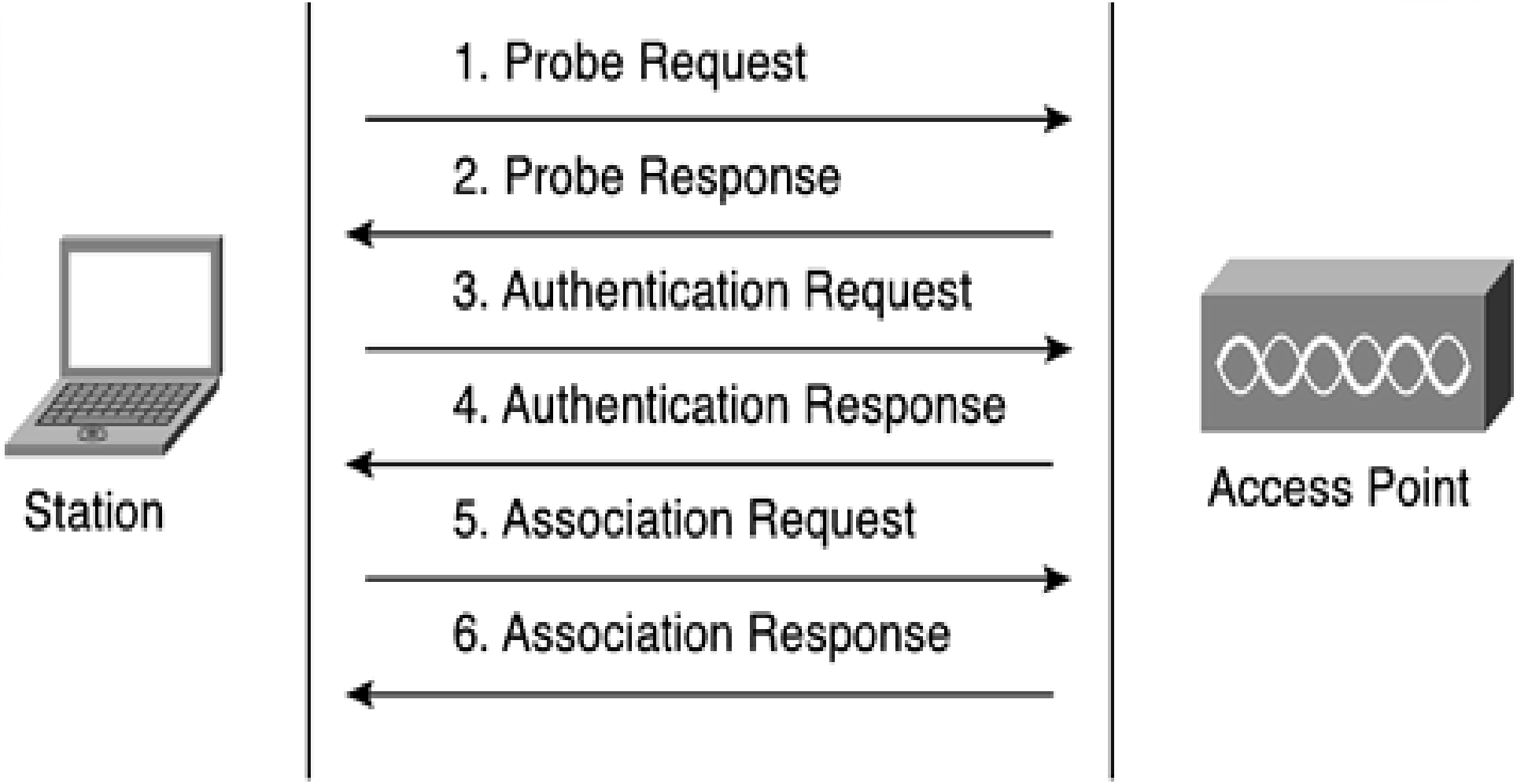
Standar WiFi

- Standar WiFi adalah 802.11 yang di mana ada berbagai versi nya dengan kecepatan dan harga yang berbeda-beda.
- 802.11b adalah yang paling lambat namun murah
- 802.11a
- 802.11g
- 802.11n adalah yang paling cepat namun mahal

Frekuensi dan Kanal

- Setiap standar memiliki standar frekuensi dan kanal tersendiri.
- Standar terbaru menggunakan 5GHz, dan beberapa kanal di dalam jangkauan 5GHz tersebut. Bisa terdapat 11 kanal dengan frekuensi yang berbeda-beda namun masih dalam standar yang telah ditetapkan
- Setiap negara memiliki standar frekuensi tersendiri, jadi pastikan konfigurasi negara telah di set di Router Anda

Proses Koneksi WIFI



Proses

- Station membroadcast sebuah frame request probe di setiap saluran yang memungkinkan station untuk cepat menemukan spesifik station via SSID atau WLAN yang berada dalam jangkauan.
- Access Point yang dijangkau merespon dengan frame response probe. Respon berasal dari access point infrastruktur BSS.
- Klien yang memutuskan AP yang terbaik untuk diakses.

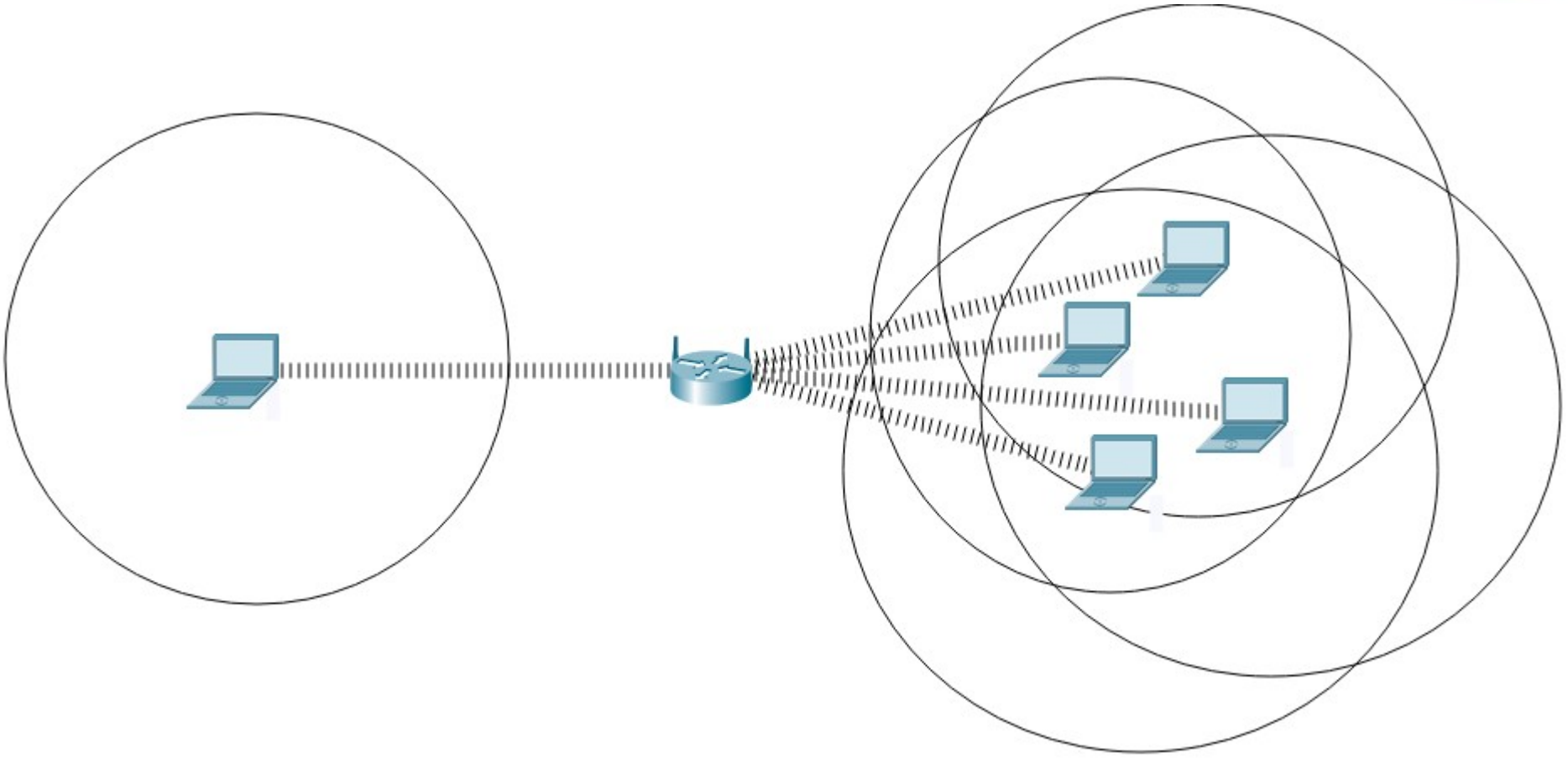
Proses

- AP mengirimkan sebuah jawaban autentikasi. Respon ini termasuk sebuah algoritma autentikasi yang dihasilkan oleh sistem.
- Setelah autentikasi berhasil, klien mengirimkan sebuah request frame kepada AP. Ini adalah langkah penting untuk memastikan keamanan pengiriman data.
- AP membalas dengan respon asosiatif.

Host Yang Tersembunyi

- Satu Host ini terletak jauh dari jangkauan dari Host-Host lainnya.
- Setiap pengiriman frame (bukan paket) diperlukan koordinasi dari tiap-tiap Host.
- Jadi jika ada Host yang tersembunyi, makan tabrakan frame bisa jadi terjadi kapanpun juga.
- Access Point biasanya bisa mengatasi ini dengan teknik RTS-CTS CTR. Atau gampangnya minta izin dulu.

Ilustrasi



Resiko Wireless

- Kerentanan SSID (SSID bisa disembunyikan)
- Kerentanan Otentifikasi
- Kerentanan Otentifikasi Berbagi
- Kerentanan Protokol WEP

Teknologi Keamanan WIFI

- Wired Equivalent Privacy (WEP)
- Wireless Protected Acess (WPA)
- WPA2 pengganti WPA (Hingga saat ini)
- Setiap Card Wireless harus bersertifikasi WIFI untuk mendukung protokol keamanan terbaru
- Router terbaru hanya mendukung Shared atau WPA atau WPA2

WPA & WPA2

- Protokol ini menggunakan teknologi *Temporary Key Integrity Protocol* dan *Advanced Encryption Standard*
- Ketika enkripsi TKIP digunakan, sebuah Message Integrity Code (MIC) diikutsertakan untuk mencegah paket dipalsukan.
- MIC menggantikan CRC dari WEP
- WPA&WPA2 ada dua jenis kunci:
  - Personal
  - Enterprise

WPA2-Personal

- Teknologi keamanan ini mengandalkan password/kata kunci sebagai keamanannya layaknya WEP
- Namun dalam proses pembuatan kuncinya tetap menggunakan teknologi enkripsi TKIP dan AES.
- Cocok untuk pengguna rumahan atau kantor kecil.

WPA2-Enterprise

- Sesuai dengan namanya, protokol ini mewajibkan penggunaan server RADIUS sebagai otentifikasi user.
- Tanpa adanya server RADIUS, user tidak bisa login menggunakan user dan password mereka
- Berbeda dengan Personal, otentifikasi dari Enterprise ini melalui dua proses yang berbeda tempat.

Ilustrasi - Personal

Ilustrasi - Enterprise

Authentication Mode:	WPA/WPA2 Enterprise ▼
Encryption Mode:	TKIP&AES ▼
RADIUS Server Address:	192.168.0.100 *
RADIUS Server Port:	1812 * (0-65535)
RADIUS Shared Key:	•••••••• ✓ Hide *