

MODUL 8 WIRELESS SECURITY

8.1 Tujuan

- Mengetahui dan memahami konsep wireless security
- Mampu mengimplementasikan konsep wireless security pada perangkat jaringan

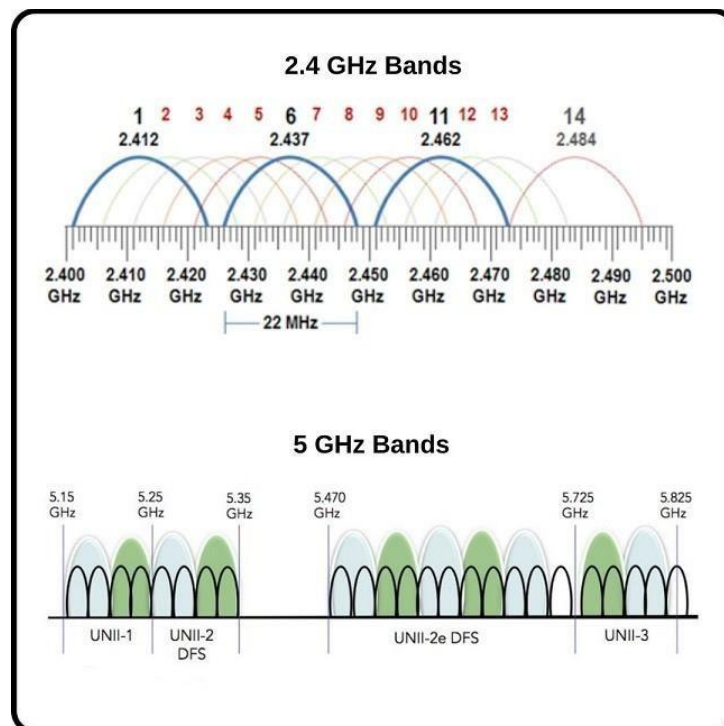
8.2 Alat dan Bahan

- Laptop
- MikroTik RB951 (Wireless)

8.3 Teori

Wi-Fi Security adalah perlindungan terhadap perangkat dan jaringan yang terhubung dalam lingkungan nirkabel. Tanpa *Wi-Fi Security*, perangkat jaringan seperti wireless access point atau router dapat diakses oleh siapa saja yang menggunakan komputer atau perangkat seluler dalam jangkauan sinyal nirkabel router tersebut. Ketika perangkat nirkabel dalam sebuah jaringan "terbuka" atau tidak aman, perangkat tersebut dapat diakses oleh perangkat yang mendukung Wi-Fi, seperti komputer atau smartphone, yang berada dalam jangkauan sinyal nirkabelnya.

Menggunakan jaringan yang terbuka atau tidak aman dapat berisiko bagi pengguna dan organisasi. Pelaku kejahatan yang menggunakan perangkat yang terhubung ke internet dapat mengumpulkan informasi pribadi pengguna, mencuri identitas, membahayakan data keuangan dan data sensitif bisnis lainnya, menyadap komunikasi, dan lain sebagainya.



Jenis-jenis protokol *wireless security*

Ada empat protokol *wireless security* utama. Protokol-protokol ini dikembangkan oleh Wi-Fi Alliance, sebuah organisasi yang mempromosikan teknologi nirkabel dan interoperabilitas. Kelompok ini memperkenalkan tiga protokol yang dijelaskan di bawah ini pada akhir tahun 1990-an. Sejak itu, protokol-protokol tersebut telah ditingkatkan dengan enkripsi yang lebih kuat. Protokol keempat dirilis pada tahun 2018.

- **WEP**

Protokol *wireless security* pertama adalah WEP (Wired Equivalent Privacy). Protokol standar untuk menyediakan keamanan jaringan nirkabel dari akhir 1990-an hingga 2004. Namun, WEP sulit dikonfigurasi dan hanya menggunakan enkripsi dasar (64-/128-bit). Saat ini, WEP tidak lagi dianggap aman dan digantikan oleh protokol yang lebih baru seperti WPA2, yang akan dijelaskan di bawah ini.

- **WPA**

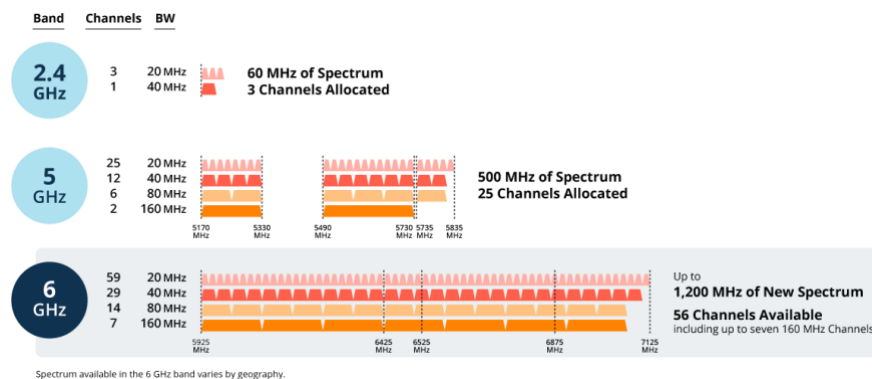
Wi-Fi Protected Access (WPA) dikembangkan pada tahun 2003. Protokol ini memberikan enkripsi yang lebih kuat (128-/256-bit) dibandingkan WEP dengan menggunakan protokol keamanan yang disebut Temporal Key Integrity Protocol (TKIP). Bersama dengan WPA2, WPA adalah salah satu protokol yang paling umum digunakan saat ini. Namun, tidak seperti WPA2, WPA kompatibel dengan perangkat lunak lama.

- **WPA2**

WPA2, versi lanjutan dari WPA, dikembangkan pada tahun 2004. Protokol ini lebih mudah dikonfigurasi dan memberikan keamanan jaringan yang lebih baik dibandingkan WPA dengan menggunakan protokol keamanan yang disebut Advanced Encryption Standard (AES). Versi protokol WPA2 tersedia untuk pengguna individu maupun perusahaan.

- **WPA3**

Generasi baru dari WPA, yang dikenal sebagai WPA3, dirancang untuk memberikan konfigurasi yang lebih sederhana dan enkripsi serta keamanan yang lebih kuat (192-/256-/384-bit) dibandingkan pendahulunya. Protokol ini juga dirancang untuk bekerja dengan jaringan Wi-Fi 6 terbaru.



Wireless Interference

Interferensi pada jaringan wireless dapat disebabkan oleh jaringan nirkabel lain, perangkat lain yang menggunakan frekuensi 2,4 GHz, dan perangkat bertegangan tinggi yang menghasilkan gangguan elektromagnetik.

- Perangkat Bluetooth seperti headphone dan speaker menggunakan frekuensi 2,4 GHz. Model Bluetooth yang terbaru biasanya dirancang untuk menghindari saluran Wi-Fi yang aktif.
- Jaringan nirkabel yang ada di sekitar, seperti yang ada di rumah tetangga, mungkin beroperasi pada frekuensi yang sama dan dapat mengganggu kinerja jaringan Wi-Fi Anda.
- Telepon nirkabel sering menggunakan frekuensi 2,4 GHz. Jika kinerja jaringan Anda menurun setiap kali telepon nirkabel digunakan, pertimbangkan untuk beralih ke telepon dengan frekuensi yang berbeda.
- Baby monitors sering menggunakan frekuensi 2,4 GHz. Mengingat koneksi yang terus-menerus antara monitor dan penerima, Baby monitors dapat memengaruhi

kinerja jaringan Anda.

- Microwave, terutama yang lebih lama atau yang memiliki pelindung yang buruk, dapat menyebabkan gangguan elektromagnetik yang cukup besar di frekuensi 2,4 GHz. Microwave yang lebih baru telah dilindungi dengan baik dan seharusnya tidak menyebabkan masalah yang signifikan.
- Peralatan wireless security seperti kamera dan sensor gerak dapat memenuhi frekuensi 2,4 GHz. Kamera dan sensor yang lebih baru sudah mendukung Wi-Fi dan dapat terhubung langsung ke jaringan Wi-Fi Anda, sehingga tidak mengganggu kinerjanya.
- Radio dan police scanner beroperasi pada berbagai frekuensi dan dapat menyebabkan gangguan pada perangkat radio lainnya yang berada di dekatnya. Kedekatan perangkat tersebut biasanya menjadi faktor penentu dalam gangguan radio, jadi sebaiknya jangan menempatkan modem Anda langsung di samping (atau di atas) perangkat pemancar radio.
- Monitor dan TV – terutama yang tidak memiliki pelindung yang memadai – dapat menyebabkan gangguan pada jaringan 2,4 GHz (khususnya pada saluran 11-14). Hindari menempatkan modem Anda langsung di samping TV, monitor, atau layar.
- Peralatan rumah tangga dengan tegangan tinggi dan konsumsi daya besar, seperti mesin cuci dan unit pendingin udara, dapat menyebabkan gangguan elektromagnetik. Jika Anda memperhatikan penurunan kinerja jaringan, Anda mungkin perlu memindahkan modem Anda lebih jauh.

