Laboratorium
Multimedia dan Internet of Things
Departemen Teknik Komputer
Institut Teknologi Sepuluh Nopember

Laporan Sementara
Praktikum Jaringan Komputer

Wired and Wireless

Ahmad Akmal Defatra - 5024231005

2025

1 Pendahuluan

1.1 Latar Belakang

Di era digital saat ini, aktivitas manusia seperti bekerja, belajar, hingga hiburan kian bergantung pada akses internet. Ketika pengguna berpindah dari satu ruangan ke ruangan lain, dari kampus ke kafe, atau dari rumah ke kantor klien, sudah menjadi standar fimana laptop dan ponsel tetap terhubung tanpa harus mencolok ke kabel jaringan atau LAN. Belum lagi lonjakan jumlah smart device seperti smartphone, tablet, jam pintar juga ditambah gelombang sensor IoT di pabrik dan perumahan, mendorong kebutuhan akan jaringan nirkabel (wireless) yang bisa diandalkan, murah dipasang, serta mudah diperluas. Maka, teknologi Wi-Fi menjadi jawabannya karena memanfaatkan media udara sehingga pemasangan cukup meletakkan access point, tanpa menarik kabel UTP ke setiap titik pengguna.

Di balik kemudahan “tanpa kabel” atau wireless, jaringan Wi-Fi sebenarnya implementasi beberapa konsep teknis penting. Gelombang radio dipancarkan pada pita 2,4 GHz dan 5 GHz yang dipecah ke area-area sempit agar sinyal antar perangkat tidak saling bertabrakan. Standar IEEE 802.11—mulai dari 802.11b berkecepatan 11 Mbps hingga Wi-Fi 6 (802.11ax) dengan teoretis 9,6 Gbps—terus berkembang memperkenalkan teknik modulasi canggih, antena MIMO, dan fitur penghemat baterai. Sementara itu, lapisan keamanan ikut berevolusi: WEP yang mudah dibobol sudah digantikan WPA2 dan kini WPA3 dengan metode autentikasi yang lebih tahan serangan. Memahami elemen-elemen ini penting agar kita dapat menilai kelebihan dan keterbatasan jaringan nirkabel dibandingkan jaringan kabel sehingga keputusan desain (misalnya backbone memakai serat optik, akses pengguna memakai Wi-Fi) dapat diambil secara tepat.

Praktikum Modul 3 memastikan memahami esensi dari praktikum dimana bukan sekadar membaca spesifikasi, tetapi mengamati langsung cara perangkat memancarkan SSID, proses klien melakukan asosiasi, hingga pengaruh pengaturan port dan enkripsi terhadap performa. Dengan demikian, setelah menyelesaikan sesi laboratorium, praktikan diharapkan mampu menilai secara kritis kapan memilih solusi nirkabel, mengenali batasannya, serta menerapkan langkah mitigasi keamanan yang memadai sebelum WLAN dilepas ke pengguna akhir.

2 Dasar Teori

2.1 Wired vs Wireless

Media kabel (Ethernet tembaga maupun serat optik) dan media nirkabel sesungguhnya menjawab kebutuhan yang berbeda. Kabel memberikan jalur fisik berpelindung sehingga sinyal elektris atau cahaya terkungkung di dalam konduktor yang membuat hasilnya latensi rendah, kecepatan konsisten, dan keamanan fisik tinggi dmana orang harus menyentuh kabel untuk menyadap jaringan. Sebaliknya, sinyal radio Wi-Fi merambat bebas di udara sehingga mudah menjangkau pengguna tanpa infrastruktur masif, namun terpapar interferensi microwave, Bluetooth, dan jaringan Wi-Fi tetangga. Memahami sifat dasar kedua media membantu administrator memilih kombinasi paling efisien: kabel bagi server dan perangkat tetap; Wi-Fi bagi staf dan tamu yang bergerak.

Tabel 1: Perbandingan wired vs wireless

Aspek	Wired	Wireless
Pemasangan	Menarik kabel/ducting	Tempatkan AP, atur kanal
Mobilitas	Terbatas panjang kabel	Bebas perpindahan dalam jangkauan
Kecepatan puncak	Up to 100Gbps (Ethernet)	Up to 9.6Gbps (Wi-Fi 6)
Latensi tipikal	<1ms LAN	2–20ms tergantung jarak
Interferensi	Minim (EMI terkontrol)	Rentan perangkat 2.4/5 GHz lain
Keamanan fisik	Tinggi (akses kabel)	Harus dienkripsi WPA2/3
Cost per node	Lebih tinggi (patch panel)	Lebih rendah; cukup NIC Wi-Fi

Meski tabel di atas menyoroti perbedaan utama, praktik terbaik di dunia nyata biasanya memadukan keduanya yang dikenal sebagai *wired backbone + wireless edge* karena kinerja stabil sekaligus fleksibilitas akses.

2.2 Standar IEEE 802.11 (Evolusi Wi-Fi)

Keluarga standar IEEE 802.11 menetapkan cara perangkat bertukar data melalui udara. Setiap revisi membawa peningkatan melalui tiga komponen: pita frekuensi, teknik modulasi, dan jumlah aliran antena.

- **802.11b** (1999) – Menyediakan 11Mbps pada pita 2.4 GHz menggunakan DSSS; mudah ditembus tembok, tapi rentan interferensi microwave.
- **802.11g** (2003) – Beralih ke OFDM di 2.4 GHz, kecepatan 54Mbps serta tetap kompatibel b.
- **802.11n** (Wi-Fi 4, 2009) – Memperkenalkan MIMO dan channel bonding 40 MHz di 2.4 & 5 GHz; dorong throughput hingga 600Mbps.
- **802.11ac** (Wi-Fi 5, 2013) – Fokus pita 5 GHz, modulasi 256-QAM, MU-MIMO downstream, lebar kanal 160 MHz; teori 6.9Gbps.
- **802.11ax** (Wi-Fi 6, 2019) – Tambah OFDMA dan TWT; bekerja di 2.4 & 5 GHz, teorinya 9.6Gbps, namun peningkatan sebenarnya terasa pada efisiensi saat banyak klien.

Sejak Wi-Fi 6E, pita 6 GHz turut dibuka, menyediakan kanal non-overlap lebih banyak sehingga kepadatan jaringan di kampus atau stadion dapat diurai tanpa berbagi kanal sempit.

2.3 Perangkat Jaringan Wireless

Jaringan WLAN terdiri dari beberapa jenis perangkat, masing-masing memainkan peran tertentu.

Access Point Perangkat Layer-2 yang memancarkan SSID dan menghubungkan klien Wi-Fi ke LAN kabel lewat port Ethernet uplink. AP bisnis mendukung PoE, VLAN tagging, dan roaming.

Wireless Router Versi SOHO yang menggabungkan router NAT, switch 4-port, DHCP, firewall, dan AP dalam satu unit yang cukup untuk rumah atau kantor kecil.

Wireless NIC Kartu jaringan pada klien (USB, PCIe, M.2) yang menangani modulasi/demodulasi sinyal RF; fitur terkini mencakup 2×2 MIMO dan 1024-QAM.

Repeater/Extender Perangkat yang menerima sinyal Wi-Fi dan memancarkan ulang untuk memperluas area liputan; menambah latensi karena proses *receive* → *transmit* berurutan.

Point-to-Point Bridge Dua radio directional (biasanya 5GHz) dalam mode bridge untuk menghubungkan dua gedung LOS sejauh beberapa kilometer tanpa menarik serat optik.

Memilih perangkat yang tepat bergantung pada skenario: jangkauan ruangan, kepadatan pengguna, dan kebutuhan kecepatan.

2.4 Keamanan WLAN

Karena sinyal Wi-Fi tersebar bebas, keamanan menjadi prioritas utama. Skema enkripsi berevolusi dari WEP (RC4 40-bit, mudah dipatahkan) ke WPA (TKIP) lalu WPA2 (AES-CCMP). WPA3 memperkenalkan **SAE** yakni prosedur handshake tahan serangan *dictionary* dan 192-bit Suite-B untuk lingkungan pemerintah. Selain enkripsi, administrator harus mengimplementasikan kebijakan berikut:

- Mengubah SSID dan kata sandi admin bawaan access-point.
- Menonaktifkan WPS tombol satu sentuh yang rentan brute-force PIN.
- Mengaktifkan *client isolation* pada jaringan publik untuk mencegah sniffing antar-pengguna.
- Memakai radius 802.1X atau setidaknya WPA2-Enterprise pada jaringan perusahaan.

Langkah-langkah tersebut, meski sederhana, menutup sebagian besar celah umum yang sering dieksploitasi peretas.

Tugas Pendahuluan

1. **Jelaskan apa yang lebih baik, jaringan wired atau jaringan wireless?**
   Jaringan *wired* baik tembaga maupun optik masih menjadi rujukan ketika prioritasnya adalah latensi mikro-detik, kestabilan throughput tanpa variasi, dan keamanan fisik tinggi. Hal ini krusial di pusat data, server penyimpanan gambar medis, dan backbone kampus yang mengalirkan trafik antarfakultas. Seperti yang diuraikan pada Tabel 1, sinyal listrik atau cahaya di dalam kabel terlindung dari interferensi gelombang lain sehingga kecepatan 1–100 Gbps dapat dipertahankan 24 jam tanpa fluktuasi ekstrem. Sebaliknya, *wireless* unggul pada fleksibilitas dimana cukup menempatkan access-point di plafon, puluhan klien langsung online tanpa menarik patch-cord dan punch-down patch-panel. Biaya instalasi ruangan lama pun berkurang drastis karena tidak perlu membongkar dinding membuat jalur kabel. tapi pilihan terbaik adalah **hibrida** (backbone kabel + akses Wi-Fi) memberi nilai paling seimbang dimana kabel menjaga performa server dan printer dan Wi-Fi menghadirkan mobilitas bagi staf, tamu, dan IoT portabel. Intinya, “lebih baik” bersifat kontekstual dan mesti diukur terhadap kebutuhan kecepatan, jumlah pengguna bergerak, serta anggaran pemeliharaan.
2. **Apa perbedaan antara router, access point, dan modem?**

Modem

Bekerja di physic-layer untuk menyesuaikan sinyal media luar (DSL, DOCSIS, GPON) menjadi Ethernet ber-IP. Ia tidak men-route paket dan biasanya menyediakan satu port RJ-45 yang diteruskan ke router. Tanpa modem (atau ONT), rumah/kampus tidak dapat "berbicara" dengan jaringan ISP.

Router

Perangkat network layer (L3) yang memutuskan ke mana paket dikirim berdasarkan tabel rute. Fitur tambahannya mencakup NAT, firewall, DHCP, QoS, dan VPN. Pada router rumah, fungsi ini sering dikemas bersama switch kecil dan AP, sehingga dikenal sebagai "wireless router".

Access-Point

Perangkat data-link layer (L2) yang memancarkan SSID dan menjembatani frame 802.11 802.3. Ia tidak melakukan NAT dimana semua paket klien diteruskan ke router untuk diproses. AP kelas enterprise mendukung VLAN tagging, roaming, PoE, dan manajemen terpusat via controller.

tambahan: modem menyiapkan jalur ke ISP, router mengelola lalu lintas IP dan meneruskan paket, sementara access-point hanya menyediakan "pintu udara" agar perangkat Wi-Fi bisa masuk ke LAN yang diatur router. Memahami pembagian peran ini mencegah kesalahan konfigurasi seperti NAT berlapis atau DHCP ganda yang kerap terjadi di jaringan kecil.

3. **Jika kamu diminta menghubungkan dua ruangan di gedung berbeda tanpa menggunakan kabel, perangkat apa yang kamu pilih? Jelaskan alasannya.**

   Pilihan utama adalah dengan Point-to-Point (PtP) Wi-Fi bridge.
   Sepasang radio directional 5GHz (mis. Ubiquiti NanoStation Loco M5 atau TP-Link CPE510) dipasang saling menghadap. Keunggulannya:

   - *Spektrum efisien* – antena sempit meminimalkan interferensi kanal 2,4 GHz yang padat.
   - *Throughput tinggi* – mode 802.11n/ac single-stream stabil 150300Mbps.
   - *Bridge transparan* – kedua ruangan tetap satu subnet, tidak perlu NAT atau routing tambahan.
   - *Biaya rasional* – total investasi < tarik fiber, instalasi cukup dudukan PoE.
   - *Keamanan terarah* – sinyal fokus + WPA2/WPA3 AES menekan risiko eavesdropping.

   Alternatif lain (bila PtP tidak tersedia):

   a) *Wi-Fi Repeater/Extender* – mudah dipasang, namun throughput efektif turun ±50
   b) *Mesh Wi-Fi Node* – dua node mesh (mis. TP-Link Deco) dapat menjembatani ruangan, otomatis memilih kanal dan membuat backhaul 5 GHz; latensi sedikit lebih tinggi dari PtP, tetapi konfigurasi lebih ramah pengguna.
   c) *PoE Access-Point + Client Bridge* – salah satu ruangan memakai AP indoor biasa, ruangan satunya dilengkapi adaptor "wireless client» (NIC USB 5 GHz atau router WISP) untuk menerima sinyal; solusi ekonomis bila LOS terhalang sebagian.

   Ketiga alternatif diambil dari perangkat yang dibahas pada sub-bab *Perangkat Jaringan Wireless* di Dasar Teori, namun PtP bridge tetap menjadi rekomendasi utama karena menawarkan kombinasi jangkauan, kestabilan, dan efisiensi kanal paling baik untuk jarak 50m LOS.