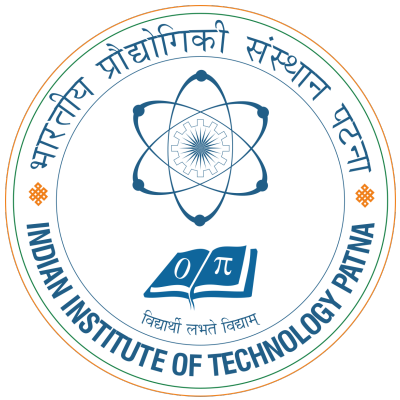
Chapter 01 Learning Objectives

Dr. Mayank Agarwal

Department of CSE
IIT Patna

CS6206 Selected Topics in Wireless Networks



Lecture 1 Learning Objectives I

By the end of this lecture, you will be able to:

- Explain the fundamental motivation and advantages of wireless networks over wired networks.
- Identify and distinguish between different categories of wireless networks (WPAN, WLAN, WWAN).
- Describe the core challenges unique to wireless communication from a networking perspective.
- Name the key standards bodies governing Wi-Fi and their primary roles.
- Outline the general structure and evolution of the 802.11 standard family.

The Big Question: Why Wireless? I

- **Freedom from Physical Tethers:** Mobility, convenience, and flexibility.
- **Infrastructure Cost & Deployment Speed:** Often cheaper and faster to deploy than running cables (Ethernet, fiber).
- **Enabling New Applications:** Mobile computing, IoT, location-based services, vehicular networks.
- **Challenging Environments:** Historic buildings, industrial sites, outdoor areas.

Key Trade-off: We trade the reliable, high-performance, secure channel of a wire for convenience and mobility, introducing a host of new problems to solve.

The Wireless Landscape: Taxonomy by Range I

- **Wireless Personal Area Network (WPAN):** ~10m
  - **Examples:** Bluetooth (802.15.1), Zigbee (802.15.4), NFC.
  - **Purpose:** Cable replacement between personal devices.
- **Wireless Local Area Network (WLAN):** ~100m
  - **Example:** Wi-Fi (IEEE 802.11). **Our Focus.**
  - **Purpose:** Local network access, extension of wired LAN.
- **Wireless Metropolitan Area Network (WMAN):** ~10km
  - **Example:** WiMAX (802.16).
  - **Purpose:** Broadband wireless access.
- **Wireless Wide Area Network (WWAN):** Country/Global
  - **Examples:** Cellular (4G LTE, 5G), Satellite.
  - **Purpose:** Ubiquitous mobile connectivity.

Evolution from Wired to Wireless Networks I

- **Ethernet (Wired LAN) Model:**
  - **Medium:** Dedicated copper/fiber link per device or switched.
  - **Access:** CSMA/CD (Carrier Sense Multiple Access with Collision Detection).
  - **Characteristics:** Full-duplex, high reliability, stable performance.
- **Wireless LAN Model:**
  - **Medium:** Shared, open radio frequency (RF) spectrum.
  - **Access:** CSMA/CA (Collision Avoidance). **Collision Detection is impossible!**
  - **Characteristics:** Half-duplex, broadcast medium, variable performance.
- **Philosophical Shift:** From "perfect link, imperfect network" to "imperfect link, smart network."

Wi-Fi Physical Layer (PHY) Concepts: The Foundation I

- **Spectrum:** The "neighborhood" of radio frequencies. Wi-Fi uses the 2.4 GHz (crowded, longer range) and 5 GHz (faster, more space) bands.
- **Channel:** A specific "lane" or frequency within a band. Routers choose one to avoid interference from neighbors.
- **Modulation:** The method of encoding data (1s and 0s) onto a radio wave, like changing a pitch or tone to carry information.
- **MIMO:** Using multiple antennas to talk and listen simultaneously, boosting speed and reliability. This is like having multiple mouths and multiple ears. They can talk to multiple devices at once (like holding two separate conversations with two people) or send multiple streams of data to one device (like splitting a movie file into parts and sending them all at the same time). This is a huge boost for speed.

Wi-Fi Physical Layer (PHY) Concepts: The Foundation II

The PHY layer is how we shout data through the air. We need to understand this to see why the MAC layer's "rules of shouting" are necessary.

Core Concept: What is a "Channel"? I

- **Band:** The overall frequency neighborhood (e.g., 2.4GHz or 5GHz).
- **Channel:** A specific, numbered frequency "address" or lane within that band.
- **Interference:** The problem when multiple networks (or devices like microwaves) use the same or overlapping channels, causing "shouting" and slowing data down.

Choosing the right channel is like picking the clearest lane on a radio highway. This is a physical-layer setup task that directly impacts MAC layer performance.

Core Concept: What is "OFDM"? (Conceptually) I

- **The Problem:** Sending data as one big, fast stream is like one large truck. Interference (a "pothole") can ruin the whole delivery.
- **The OFDM Solution:** Splits the data into many slow, small streams sent in parallel over closely spaced, non-interfering sub-lanes.
- **The Benefit:** Robustness. If interference hits a few sub-lanes, only small pieces of data are affected and can be re-sent. The rest get through. This is key to reliable high-speed Wi-Fi.

OFDM (Orthogonal Frequency Division Multiplexing) is the PHY layer's clever traffic management system that prevents total failure from small amounts of interference.

From PHY to MAC: The Complete Picture I

- **Physical (PHY) Layer:** How to shout. Defines the spectrum, channels, modulation (OFDM), and hardware (MIMO).
- **MAC (Media Access Control) Layer:** The rules for shouting. Manages access to the shared channel to prevent collisions.

The MAC layer performs critical functions based on PHY conditions:

- **Carrier Sense:** "Listen before you talk" to avoid collisions.
- **Collision Recovery:** Back-off rules if two devices transmit simultaneously.
- **Addressing & Framing:** Packages data with correct source/destination info.

You need a robust PHY (good highways) for an efficient MAC (good traffic laws) to work effectively.

Core Challenge 1: The Shared, Open Medium I

- **Broadcast Nature:** Every transmission is heard by all devices within range.
  - **Implication:** Security is paramount (encryption, authentication).
  - **Implication:** Efficient use requires coordination.
- **Unlicensed Spectrum:** Operates in ISM (Industrial, Scientific, Medical) bands.
  - **2.4 GHz:** Crowded (Wi-Fi, Bluetooth, microwaves, cordless phones).
  - **5 GHz:** More channels, less crowded (historically).
  - **6 GHz:** Newest band (Wi-Fi 6E/7), very wide channels.
- **Interference:** Non-Wi-Fi devices (microwaves) and other Wi-Fi networks compete for the same spectrum.

Analogy: Like holding a conversation in a crowded, noisy room where everyone speaks the same language.

Core Challenge 2: The Hidden & Exposed Node Problems I

Problem Definition: In wireless, "carrier sense" is local; a node cannot always hear what its intended receiver can hear.

- **Hidden Node:** Node A and Node C cannot hear each other, but both can communicate with Node B. A and C may transmit simultaneously, causing a collision at B.
- **Exposed Node:** Node B is transmitting to A. Node C, hearing B's transmission, refrains from transmitting to D, even though C$\rightarrow$D would not interfere with B$\rightarrow$A.

Networking Impact: These problems drastically reduce spatial reuse and throughput. Solutions require protocol mechanisms (RTS/CTS) at the MAC layer.

Core Challenge 3: Dynamic Channel Conditions I

- **Path Loss:** Signal strength decreases with distance ($\propto 1/d^n$, where n is the path loss exponent, typically 2-4).
- **Multipath Fading:** Signals reflect off objects, creating multiple paths that can constructively or destructively interfere at the receiver.
- **Doppler Shift:** Frequency shift due to relative motion between transmitter and receiver.

Networking Impact: The "link quality" is not binary (up/down) but a continuous variable (SNR). This demands:

- Adaptive modulation and coding (PHY rate adaptation).
- Robust retransmission strategies.
- Handoff decisions for mobile clients.

Core Challenge 4: Mobility I

- **Seamless Handoff/Roaming:** A client moving between Access Points (APs) must re-associate with minimal disruption to active sessions (e.g., VoIP call, video stream).
- **Network Discovery:** The client must efficiently find new APs to connect to.
- **State Synchronization:** Security context (keys), QoS policies, and filtering rules must potentially be transferred between APs.

This is a network-layer and above challenge, requiring support from protocols beyond just 802.11 (e.g., 802.11r for Fast Transition, ICMP Router Discovery).

The Standards Ecosystem: Who Makes Wi-Fi? I

- **IEEE 802.11 Working Group:**
  - **Role:** Creates the technical standard. Defines PHY and MAC layers.
  - **Output:** The 802.11-2020 document (and amendments like 802.11ax).
  - **Focus:** Technical correctness, interoperability at the protocol level.
- **Wi-Fi Alliance (WFA):**
  - **Role:** Industry consortium that drives adoption. Performs certification.
  - **Output:** The "Wi-Fi" trademark, certification programs (WPA3, Wi-Fi 6, Easy Connect).
  - **Focus:** User experience, multi-vendor interoperability, market requirements.
- **IETF (Internet Engineering Task Force):**
  - **Role:** Defines protocols that run **over** Wi-Fi (IP, TCP) or manage it (CAPWAP for AP control).
  - **Output:** RFCs (Requests for Comments).

The Standards Ecosystem: Who Makes Wi-Fi? II

Analogy: IEEE writes the dictionary and grammar (802.11), WFA ensures everyone speaks the language fluently and compatibly (Wi-Fi Certified), IETF defines the conversations we have using that language (IP networking).

A Brief History of 802.11: The Timeline I

- **1997 (802.11 legacy):** The original standard. 2.4 GHz, 1-2 Mbps (FHSS, DSSS).
- **1999 (802.11b):** 2.4 GHz, up to 11 Mbps (DSSS/CCK). First mass-market success.
- **1999 (802.11a):** 5 GHz, up to 54 Mbps (OFDM). Ahead of its time.
- **2003 (802.11g):** 2.4 GHz, up to 54 Mbps (OFDM). Backwards compatible with 'b'.
- **2009 (802.11n - Wi-Fi 4):** MIMO, 40 MHz channels, frame aggregation. Major leap.
- **2013 (802.11ac - Wi-Fi 5):** 5 GHz only, wider channels (80/160 MHz), MU-MIMO (downlink).
- **2019 (802.11ax - Wi-Fi 6/6E):** OFDMA, Uplink MU-MIMO, BSS Coloring, 6 GHz band.

A Brief History of 802.11: The Timeline II

- **2024+ (802.11be - Wi-Fi 7):** Multi-Link Operation (MLO), 320 MHz channels, multi-AP coordination.

The 802.11 Protocol Stack (Simplified OSI Mapping) I

- **Application/Presentation/Session (Layers 5-7):** HTTP, SMTP, DNS, etc. (IETF domain).
- **Transport (Layer 4):** TCP, UDP (IETF domain). Wireless impacts TCP performance significantly.
- **Network (Layer 3):** IP (IETF domain). Wi-Fi is a Layer 2 technology.
- **Data Link Layer (Layer 2): IEEE 802.11 Domain**
  - **Logical Link Control (LLC - 802.2):** Standard interface to upper layers.
  - **Medium Access Control (MAC - 802.11): CORE OF OUR COURSE.** Framing, addressing, channel access (CSMA/CA), error control, security.
- **Physical Layer (Layer 1 - PHY - 802.11):** Modulation, coding, OFDM, MIMO. We cover concepts, not implementation.

The 802.11 Protocol Stack (Simplified OSI Mapping) II

Course Focus: The 802.11 MAC and its interaction with the PHY and upper layers (Layers 2 & 3).

Key Networking Concepts: CSMA/CA vs. CSMA/CD I

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) - Ethernet:

- **Listen** while transmitting.
- If a collision is **detected**, stop, send jam signal, wait (backoff), retry.
- Works because signal strength is high on a wired link.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) - Wi-Fi:

- **Cannot** reliably detect a collision while transmitting. Why?
  1. Transmitter's own signal drowns out others (near-far problem).
  2. Hidden node problem.
- Therefore, must **avoid** collisions proactively.
- Uses a **three-way handshake** (RTS-CTS-Data-ACK) and **random backoffs** before transmitting.

This fundamental difference shapes the entire MAC design.

Key Networking Concepts: The Basic Service Set (BSS) I

The fundamental building block of an 802.11 network.

- **Independent BSS (IBSS):** An ad-hoc network. Peer-to-peer, no central coordinator. Rare in practice.
- **Infrastructure BSS:** The common model.
  - One central **Access Point (AP)** acts as a bridge to the wired network.
  - Multiple wireless **stations (STAs)** associate with the AP.
  - All communication goes through the AP (even STA-to-STA).
  - The AP's identity is its **BSSID** (a MAC address).
- **Extended Service Set (ESS):** Multiple APs with the same **SSID** (network name) connected via a **Distribution System (DS)** - typically a switched Ethernet LAN. Enables roaming.

Think of: BSS = One cell, ESS = The entire campus Wi-Fi network.

Numerical Example 1: Transmission Time Calculation I

Problem: An 802.11ac AP transmits a 1500-byte data frame (IP packet) to a client using a PHY rate of 433 Mbps. Ignoring MAC overhead, preambles, and waiting times, how long does the transmission of the data portion itself take over the air?

Solution Steps:

1. Convert packet size to bits: 1500 bytes $\times 8$ bits/byte $= 12,000$ bits.
2. Time = Size / Rate. Use consistent units.
3. Rate = 433 Mbps = 433×10^6 bits per second.
4. Time $= \dfrac{12,000 \text{ bits}}{433 \times 10^6 \text{ bps}} = 2.77 \times 10^{-5}$ seconds.
5. Convert to microseconds (μs): 2.77×10^{-5} s $\times 10^6 \mu s/s = 27.7 \mu s$.

Numerical Example 1: Transmission Time Calculation II

Model Answer: The raw data transmission takes approximately $\mathbf{27.7}$ $\mu\mathbf{s}$.
Reality Check: Actual airtime will be 2-4x longer due to ACK frames, protocol headers, and inter-frame spacing. This is the PHY payload time only.

Numerical Example 2: Capacity vs. Coverage I

Scenario: You are designing Wi-Fi for a lecture hall (50m x 30m). You can install:

- **Option A:** 1 powerful AP in the center, max PHY rate 867 Mbps (to a single client under ideal conditions).
- **Option B:** 4 smaller APs (one in each quadrant), each with max PHY rate 433 Mbps.

Question: Which design likely provides better **aggregate throughput** for 40 simultaneous clients? Why?

Model Answer: Option B (4 APs) is superior for aggregate throughput.

- **Reason 1 (Spatial Reuse):** Four APs can transmit **simultaneously** on four different, non-overlapping channels (e.g., 1, 6, 11, 36). The single AP design has only one channel.

Numerical Example 2: Capacity vs. Coverage II

- **Reason 2 (Load Distribution):** 40 clients share the medium. With one AP, they all contend for time on one channel. With four APs, clients are distributed, reducing contention per channel.
- **Reason 3 (Link Rate):** Clients are closer to their respective APs, likely maintaining a higher PHY rate (closer to the max 433 Mbps) than clients at the edges of the single AP's large cell.

Trade-off: Option B has higher cost/complexity (multiple APs, channel planning, wired backhaul).

Numerical Example 3: The Cost of Overhead I

Problem: Assume an 802.11n transmission. The MAC/PHY headers and preamble total 40 μs of airtime. The ACK takes 20 μs. The mandatory waiting time (DIFS) before transmitting is 34 μs. Using the 1500-byte frame from Example 1 at 433 Mbps (27.7 μs data time):

- What is the total airtime for one successful data frame transmission?
- What is the protocol efficiency (data time / total time)?

Solution Steps:

1. Sum all components: DIFS + Header/Preamble + Data + SIFS + ACK.
2. Assume SIFS = 16 μs (typical).
3. Total time = $34 + 40 + 27.7 + 16 + 20 = 137.7\ \mu s$.
4. Efficiency = $\frac{27.7}{137.7} \approx 0.201 = 20.1\%$.

Numerical Example 3: The Cost of Overhead II

Model Answer: Total airtime $\approx \mathbf{138}\ \mu\mathbf{s}$. Protocol efficiency $\approx \mathbf{20}\%$.
Key Insight: Overhead dominates! This is why later standards (n, ac, ax) introduced **frame aggregation** (sending multiple packets in one burst) to amortize overhead and boost efficiency to 70-80%.

Important Terminology 1: Frames, Packets, Datagrams I

- **Frame (Layer 2):** The unit of data transmitted over a single hop. Contains source/destination MAC addresses and error checking (FCS). In 802.11, there are Management, Control, and Data frames.
- **Packet (Layer 3):** The unit of data routed across a network (e.g., an IP packet). A packet is **encapsulated** inside a frame for delivery over a link.
- **Datagram:** Often synonymous with packet, especially in connectionless protocols like UDP/IP.

Flow: Application Data $\rightarrow$ TCP Segment / UDP Datagram $\rightarrow$ IP Packet $\rightarrow$ 802.11 Data Frame $\rightarrow$ PHY Symbols.

Important Terminology 2: Bandwidth vs. Throughput I

- **Bandwidth (Channel Width):** The width of the RF channel in MHz (e.g., 20, 40, 80 MHz). A wider channel provides a larger "pipe."
- **PHY Rate (Data Rate, Link Speed):** The maximum theoretical speed at the PHY layer, in Mbps or Gbps (e.g., 433 Mbps, 1.2 Gbps). Determined by modulation, coding, channel width, and number of spatial streams. **Advertised on the box.**
- **Throughput (Goodput):** The actual application-level data transfer rate, measured in Mbps. This is what you experience.
  - Throughput $\approx$ PHY Rate $\times$ Protocol Efficiency $\times$ (1 - Contention Factor).
  - Typically 50-70% of PHY rate in good conditions, can drop much lower with many clients.

Example: An 802.11ac AP with a 1.3 Gbps PHY rate might deliver real TCP throughput of about 800 Mbps to a single client in ideal, isolated conditions.

Important Terminology 3: Latency & Jitter I

- **Latency (Delay):** The time for a packet to travel from source to destination.
  - **Air-time Latency:** Time spent transmitting/retransmitting over the wireless link.
  - **Contention Latency:** Time spent waiting for the medium to be free (backoff).
  - **Queuing Latency:** Time spent in buffers at the AP or client.
- **Jitter:** Variation in latency. Critical for real-time applications (VoIP, video conferencing, gaming).

Wireless Impact: Both latency and jitter are higher and more variable than on wired Ethernet due to the shared, unreliable medium and retransmissions. Wi-Fi 6 (802.11ax) introduces features like OFDMA and TWT specifically to improve latency.

Common Wi-Fi Deployment Models I

- **Home/Small Office (SOHO):**
  - Single AP, often a combo device (router/switch/AP).
  - Little to no channel planning.
  - Security: WPA2-Personal (Pre-Shared Key).
- **Enterprise/Campus:**
  - Many APs, centrally managed (wireless controller).
  - Careful channel and power planning (RF site survey).
  - Security: WPA2/3-Enterprise (802.1X/RADIUS).
  - Advanced features: Roaming, QoS, guest access, intrusion detection.
- **Carrier/Public Hotspot:**
  - High-density (airports, stadiums). on captive portals, billing, and seamless authentication (Passpoint/Hotspot 2.0).
- **Mesh Networks:**
  - APs connect wirelessly to each other to extend coverage where cabling is difficult.
  - Uses 802.11s protocol or proprietary implementations.

Thinking Like a Wireless Network Engineer I

Key design questions:

1. **Coverage or Capacity?** Is the goal to cover a large area with a basic signal, or to support many high-bandwidth users in a dense area? (They often conflict).
2. **2.4 GHz or 5/6 GHz?** 2.4 GHz has better range but fewer channels and more interference. 5/6 GHz has more channels, less interference, but shorter range.
3. **Channel Planning:** Assign non-overlapping channels to neighboring APs to minimize co-channel interference. **Golden Rule for 2.4 GHz:** Use only channels 1, 6, and 11 (in the US).
4. **Client Density:** How many devices will associate per AP? This drives the need for more, lower-power APs (capacity design).

Takeaway: Wireless network design is an optimization problem with multiple, often competing, constraints.

Security: A First Look I

Wireless's broadcast nature makes security non-optional.

- **Authentication:** Who is allowed to join the network?
  - **Personal (PSK):** A single password shared by all users.
  - **Enterprise (802.1X):** Individual user credentials (username/password, certificate).
- **Confidentiality/Encryption:** Preventing eavesdropping.
  - **WPA2:** Uses AES-CCMP. Considered secure with a strong password.
  - **WPA3:** Adds SAE (for PSK) and mandatory encryption for open networks (OWE).
- **Integrity:** Ensuring packets are not altered in transit (provided by the encryption protocol).

Never use: Open networks (no security) or WEP (broken within minutes). Default to WPA2-Personal (AES) at a minimum, WPA3 if supported.

Looking Ahead: Wi-Fi 6/6E and Wi-Fi 7 I

The future is about efficiency in dense, high-demand environments.

- **Wi-Fi 6 (802.11ax):** "High Efficiency" Wireless.
  - **OFDMA:** Shares a channel among multiple users simultaneously (like cellular).
  - **Target Wake Time (TWT):** Schedules client wake-ups to save battery (IoT).
  - **BSS Coloring:** Labels frames to ignore interference from distant APs.
- **Wi-Fi 6E:** Adds operation in the new 6 GHz band (massive amount of spectrum).
- **Wi-Fi 7 (802.11be):** "Extremely High Throughput."
  - **Multi-Link Operation (MLO):** A device can use 2.4, 5, *and* 6 GHz bands simultaneously for aggregation or failover.
  - **320 MHz Channels:** Even wider channels (in 6 GHz).
  - **Multi-AP Coordination:** APs can cooperate to serve clients, not just compete.

Summary: Key Takeaways from Lecture 1 I

1. Wireless networks trade the reliability of wires for mobility and convenience, introducing unique challenges: shared medium, hidden/exposed nodes, dynamic channels, and mobility.
2. The 802.11 (Wi-Fi) standard governs WLANs. Development is split between IEEE (technical standards) and the Wi-Fi Alliance (certification & branding).
3. The core networking challenge is managing access to a shared, half-duplex, unreliable broadcast medium using CSMA/CA.
4. Performance metrics (Throughput, Latency, Jitter) are heavily influenced by protocol overhead, contention, and interference, not just the PHY rate.
5. Modern Wi-Fi evolution (Wi-Fi 6/7) focuses on spectral efficiency and performance in dense deployments, not just peak speed.

Reading & Preparation for Next Lecture I

- **Required Reading:**
  - Textbook (Gast): Chapter 1 - "Introduction to Wireless Networking".
  - Review the OSI model and Ethernet (CSMA/CD) from your prerequisites.
- **Optional/Advanced Reading:**
  - IEEE 802.11-2020 Standard: Clause 4 ("General description") – available via IEEE Xplore (library).
  - Wi-Fi Alliance website: `https://www.wi-fi.org/`
- **Next Lecture (Lecture 2): Radio Fundamentals for CS Students**
  - We will cover **just enough** PHY layer concepts to understand MAC layer operation: spectrum, channels, modulation, MIMO. No heavy math.
  - Be prepared to discuss: What is a "channel"? What does "OFDM" mean at a conceptual level?

Review Questions I

Test your understanding:

1. What is the primary reason CSMA/CD cannot be used in Wi-Fi?
2. Explain the hidden node problem in your own words.
3. A client sees two Wi-Fi networks named "CampusWiFi." Is this one ESS or two? What determines the answer?
4. If an 802.11ac link has a PHY rate of 867 Mbps, what is a realistic maximum TCP throughput you could expect? Why?
5. What are the two main roles of the Wi-Fi Alliance, and how do they differ from the IEEE's role?

Discussion Question for Tutorial: "In a future smart city, everything from streetlights to sensors to autonomous cars will use wireless. Which of the fundamental wireless challenges discussed today will be the most critical to solve for that scenario, and why?"

Appendix: Useful Constants & Conversions I

- 1 Byte (B) = 8 bits (b)
- 1 Megabit per second (Mbps) = 1×10^6 bits per second (bps)
- 1 Gigabit per second (Gbps) = 1×10^9 bps
- 1 microsecond (μs) = 1×10^{-6} seconds
- 1 millisecond (ms) = 1×10^{-3} seconds = 1000 μs
- Typical 802.11 Inter-Frame Spaces:
  - SIFS: 10 μs (2.4 GHz) / 16 μs (5 GHz)
  - DIFS: SIFS + (2 $\times$ Slot Time). Slot Time varies (e.g., 9 μs for 802.11ac 5 GHz $\rightarrow$ DIFS = 16 + 18 = 34 μs).
- Speed of Light (c): 3×10^8 m/s. (Useful for later discussions on antenna spacing in MIMO).

Thank you!

Thank you!