

UNIT 2

The Network Infrastructure for E-Commerce & Wireless Application Protocol

(8 Hours) — MIS and E-Business (CACS301)

2.1 Introduction to the Information Superhighway (I-Way)

The Information Superhighway, commonly abbreviated as the I-Way, refers to the vast, interconnected web of communication networks, computers, databases, and consumer electronics that together deliver vast amounts of information to users at high speed. It is the underlying digital infrastructure that makes Electronic Commerce possible — carrying voice, video, and data traffic across telephone lines, cable networks, satellite links, and fibre-optic backbones to connect businesses, governments, and individuals around the globe.

The I-Way is not a single network but a "network of networks" built by linking together local networks, regional networks, national backbones, and international gateways. It provides the physical and logical pathway over which e-commerce transactions — browsing, ordering, payment, and delivery of digital goods — actually travel. Just as a physical highway system allows vehicles to move goods between cities, the I-Way allows electronic packets of information to move between any two connected points on Earth.

Note: Think of the I-Way as the electronic equivalent of the interstate highway system — it supplies the on-ramps, lanes, and traffic-control mechanisms that let information travel efficiently from source to destination.

2.2 Components of the I-Way

The I-Way is generally described using a three-tier conceptual model, along with the standards and regulatory framework that ties the tiers together. Figure 2.1 illustrates how consumer devices connect through local access points to a shared global backbone, which in turn links to service and content providers under a common set of protocols and regulations.

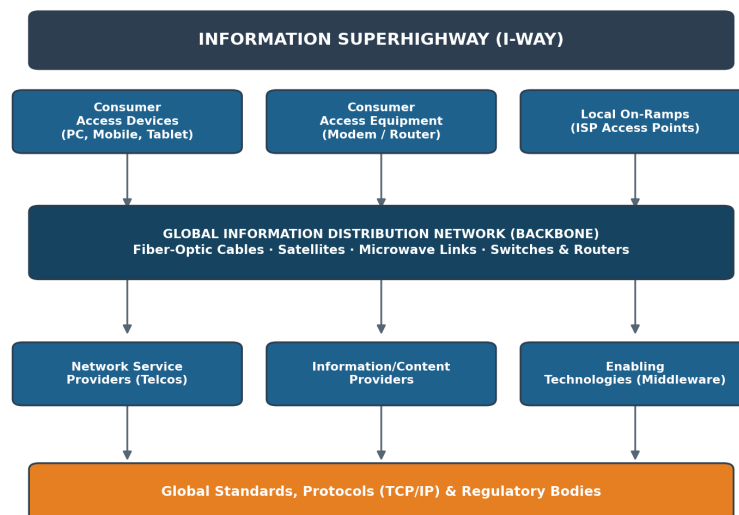


Figure 2.1: Conceptual layered structure of the Information Superhighway (I-Way)

2.2.1 Consumer Access Equipment (On-Ramps)

These are the devices and local connections that individual users employ to gain access to the network — personal computers, smartphones, tablets, modems, routers, and set-top boxes. This tier also includes "local on-ramps" such as an ISP's dial-up, DSL, cable, or wireless access point through which the consumer's traffic first enters the wider network.

2.2.2 Global Information Distribution Network (The Backbone)

This is the high-capacity core of the I-Way — fibre-optic cables, communication satellites, microwave relay links, and high-speed switches/routers that carry aggregated traffic between cities, countries, and continents. The backbone is engineered for very high bandwidth and reliability since it must simultaneously carry the combined traffic of millions of end users.

2.2.3 Network Service Providers, Content Providers & Enabling Technologies

- Network Service Providers (NSPs / Telcos): Own and operate the physical transmission infrastructure and sell bandwidth/connectivity.
- Information / Content Providers: Organisations and individuals who supply the actual data, applications, and services carried over the network (websites, portals, streaming services).
- Enabling Technologies (Middleware): Software components — protocol converters, encryption tools, directory services — that make it possible for heterogeneous hardware and networks to interoperate seamlessly.

2.2.4 Standards, Protocols & Regulation

Underlying every tier of the I-Way is a common set of technical standards (most importantly the TCP/IP protocol suite) and a regulatory framework set by national and international bodies. These standards guarantee that data originating on one type of network (say, a mobile carrier's network) can be correctly interpreted and delivered by a completely different type of network (say, a corporate LAN) anywhere else in the world.

2.3 Internet as a Network Infrastructure

The Internet is the most visible and widely used realisation of the I-Way concept. It is a global system of interconnected computer networks that uses the standard TCP/IP protocol suite to link devices worldwide. From an e-commerce perspective, the Internet supplies the common, low-cost, non-proprietary infrastructure over which businesses can reach customers, suppliers, and partners without needing to build private, dedicated networks.

2.3.1 Key Structural Elements of the Internet

- **Backbone Networks:** Extremely high-capacity long-distance links (often fibre-optic) operated by large carriers, forming the Internet's central data highways.
- **Internet Service Providers (ISPs):** Organisations that connect end users and businesses to the backbone, providing the 'last mile' of access.
- **Internet Exchange Points (IXPs):** Physical locations where different networks interconnect and exchange traffic directly, improving speed and reducing cost.
- **Routers & Switches:** Devices that direct data packets along the most efficient available path toward their destination using dynamic routing protocols.
- **Domain Name System (DNS):** A distributed directory service that translates human-readable domain names (e.g. `www.example.com`) into numeric IP addresses.

2.3.2 Why the Internet Suits E-Commerce

- Open, non-proprietary standards (TCP/IP, HTTP/HTTPS) allow any compliant device to participate.
- Global reach at comparatively low incremental cost compared to private leased-line networks.
- Packet-switching allows efficient, resilient sharing of network capacity among many simultaneous users.
- A mature ecosystem of web servers, browsers, payment gateways, and security protocols (SSL/TLS) already exists.

Note: While 'I-Way' is the broader conceptual term covering all forms of high-speed information infrastructure (including private and satellite networks), the public Internet is today the dominant

2.4 Wireless Application Protocol (WAP)

As mobile phones became capable of more than voice calls, there was a need for a standard that would let these resource-constrained handheld devices — with small screens, limited memory, and low-bandwidth wireless links — access Internet-style content and services. The Wireless Application Protocol (WAP) was developed as an open, global standard to bring web-like browsing, e-mail, and simple transactional services to mobile phones and other wireless terminals.

- WAP defines a complete communication protocol stack, purpose-built for the constraints of wireless networks (low bandwidth, high latency, small displays, limited processing power).
- It uses WML (Wireless Markup Language) instead of full HTML, and WMLScript instead of JavaScript, to keep content lightweight.
- WAP is maintained by the Open Mobile Alliance (OMA), formed from the original WAP Forum.

2.4.1 Architecture of WAP

The WAP architecture is organised as a layered protocol stack, closely mirroring the structure of the familiar Internet stack but re-engineered for the wireless environment. Each layer offers a well-defined service to the layer above it and can be replaced independently as underlying bearer technologies evolve. Figure 2.2 shows the complete stack from the application layer down to the physical bearer network.

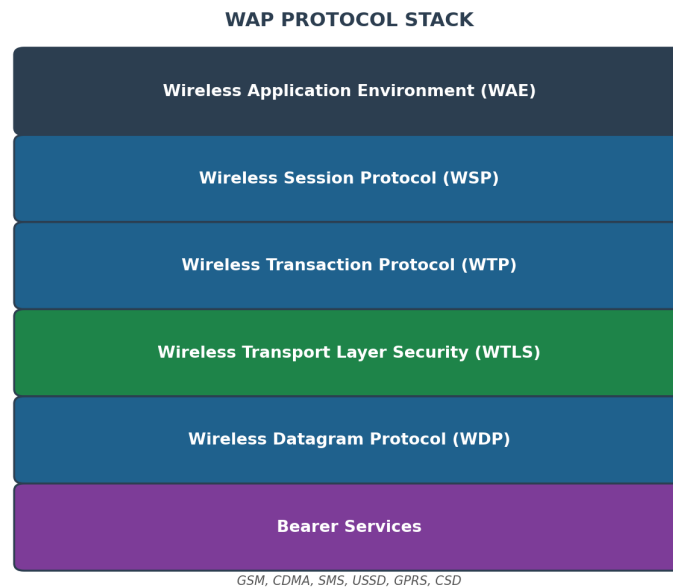
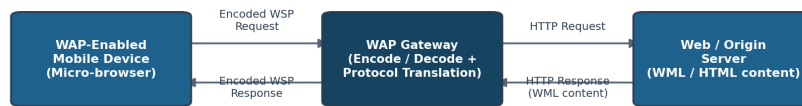


Figure 2.2: The WAP Protocol Stack, from the application layer down to the bearer network

Layer	Protocol	Function
Application	Wireless Application Environment (WAE)	Micro-browser, WML content, WMLScript, WTA (Wireless Telephony Application)
Session	Wireless Session Protocol (WSP)	Establishes/suspends/resumes sessions between client and gateway
Transaction	Wireless Transaction Protocol (WTP)	Manages reliable request-response transactions
Security	Wireless Transport Layer Security (WTLS)	Provides encryption, data integrity, and authentication
Transport	Wireless Datagram Protocol (WDP)	Adapts upper layers to whichever bearer network is in use
Bearer	GSM, CDMA, SMS, USSD, GPRS, CDPD	The actual physical wireless network carrying the data

2.4.2 Working of WAP

WAP operates on a client–gateway–server model. Because a mobile handset cannot efficiently process full HTML/HTTP traffic, an intermediary called the WAP Gateway sits between the handset and the ordinary web server, translating between the compact wireless protocols and standard Internet protocols. Figure 2.3 illustrates the request-response cycle.



The WAP Gateway converts compact binary WSP requests from the handset into standard HTTP requests for the web server, and translates the HTML/WML response back into an encoded form optimized for low-bandwidth wireless links.

Figure 2.3: The WAP request/response cycle through the WAP Gateway

Example: A typical WAP browsing session

1. The user's WAP-enabled phone sends an encoded WSP request for a page to the WAP Gateway.
2. The Gateway translates this into a standard HTTP request and forwards it to the origin web server.
3. The web server returns the requested content (often authored directly in WML, or converted to WML by a filter).
4. The Gateway encodes this response into a compact binary form and transmits it back over the wireless bearer.
5. The handset's micro-browser decodes and renders the WML content on the small screen.

Note: The WAP Gateway is a critical trust boundary: because content is decrypted and re-encrypted at the gateway (a limitation sometimes called the 'WAP Gap'), the gateway operator briefly has access to unencrypted data even when WTLS and SSL/TLS are both used end-to-end on either side.

2.5 Wireless Technologies

A range of wired and wireless broadband technologies underpin modern e-commerce access, spanning short-range wireless LANs to nationwide cellular networks. Each technology represents a different trade-off between coverage area, achievable speed, mobility support, and cost.

2.5.1 ADSL (Asymmetric Digital Subscriber Line)

ADSL is a wired broadband technology that transmits digital data over existing copper telephone lines. It is asymmetric because it allocates more bandwidth to the downstream direction (Internet-to-user) than to the upstream direction (user-to-Internet), which suits typical usage patterns such as web browsing and streaming where users download far more than they upload. ADSL allows simultaneous voice and data use on the same line via frequency-division multiplexing.

2.5.2 WiMAX (Worldwide Interoperability for Microwave Access)

WiMAX, standardised under IEEE 802.16, is a wireless broadband technology designed to provide metropolitan-area coverage — it is the principal technology behind WMAN (Wireless Metropolitan Area Network) deployments. WiMAX can deliver last-mile broadband access over distances of several kilometres, making it useful for connecting whole neighbourhoods or rural areas where laying cable is impractical.

2.5.3 WLAN (Wireless Local Area Network) and Wi-Fi

A WLAN links devices within a limited area — a home, office, or campus — without physical cabling, using radio waves in unlicensed spectrum bands. Wi-Fi (based on the IEEE 802.11 family of standards) is the dominant commercial brand and implementation of WLAN technology, offering high throughput over short-to-medium range and now used almost universally for local wireless Internet access.

2.5.4 WMAN (Wireless Metropolitan Area Network)

A WMAN extends wireless coverage across an entire city or metropolitan region, bridging the gap between short-range WLANs and wide-area cellular networks. WiMAX is the most common enabling technology for WMAN, though other proprietary and licensed-spectrum solutions also exist.

2.5.5 Cellular Generations: UMTS (3G), LTE (4G), and 5G NR

- UMTS (3G — Universal Mobile Telecommunications System): Introduced true mobile broadband, enabling video calls, mobile internet browsing, and richer WAP/web content on handsets.
- LTE (4G — Long-Term Evolution): An all-IP packet-switched network offering significantly higher speeds and lower latency, enabling smooth video streaming, app-based e-commerce, and mobile payments.
- 5G NR (New Radio): The current generation, offering very high peak speeds, ultra-low latency, and massive device density — supporting emerging applications such as IoT-driven commerce, AR/VR shopping, and real-time analytics at the network edge.

Figure 2.4 compares representative peak data rates across these technologies on a logarithmic scale, illustrating the dramatic growth in wireless capacity from ADSL-era fixed broadband through to 5G.

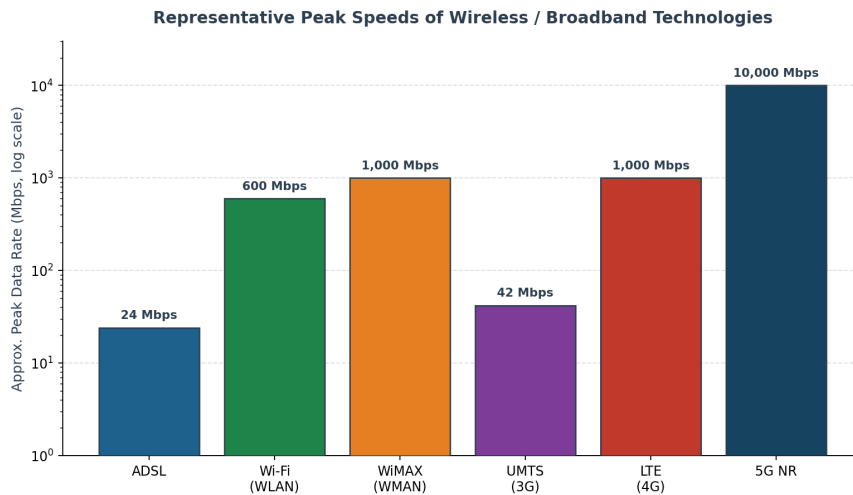


Figure 2.4: Representative peak data rates of common wireless / broadband technologies (log scale)

Technology	Typical Coverage	Mobility Support	Primary Use Case
ADSL	Fixed line (local loop)	None (fixed)	Home / office broadband Internet
Wi-Fi (WLAN)	Tens of metres	Low (local roaming)	Indoor/local wireless networking
WiMAX (WMAN)	Several kilometres	Moderate	Metro / rural broadband access
UMTS (3G)	Cell/regional	High	Mobile browsing, video calls
LTE (4G)	Cell/regional/national	High	Mobile broadband, streaming, m-commerce
5G NR	Cell/regional/national	High	IoT, AR/VR, ultra-low-latency commerce

2.6 Security Issues Related to Wireless Communications

Because wireless signals travel through open air rather than shielded cables, wireless communication introduces security risks that wired networks do not face to the same degree. Securing wireless e-commerce access requires attention to the following threats and countermeasures.

2.6.1 Common Threats

- **Eavesdropping / Interception:** Radio signals can be captured by anyone within range using inexpensive equipment, exposing unencrypted data.
- **Rogue Access Points:** Unauthorised or fake Wi-Fi access points can trick users into connecting, allowing attackers to intercept or manipulate traffic.
- **War Driving / War Walking:** Systematically scanning an area to locate unsecured or weakly secured wireless networks.

- **Man-in-the-Middle (MITM) Attacks:** An attacker secretly intercepts and possibly alters communications between two parties who believe they are communicating directly.
- **Denial-of-Service (DoS):** Jamming radio frequencies or flooding a wireless network with traffic to disrupt legitimate access.
- **Weak Encryption Protocols:** Older standards such as WEP have well-known cryptographic weaknesses that can be broken quickly with modern tools.
- **The 'WAP Gap':** The brief moment of plaintext exposure at the WAP Gateway where WTLS-encrypted traffic is translated to/from SSL/TLS.

2.6.2 Countermeasures and Best Practices

- Use strong, modern encryption standards (e.g. WPA2/WPA3 for Wi-Fi, WTLS with strong cipher suites for WAP).
- Enforce mutual authentication between client and network/gateway before establishing a session.
- Regularly update firmware and security patches on access points, gateways, and handsets.
- Deploy Virtual Private Networks (VPNs) for sensitive transactions over public wireless networks.
- Use end-to-end application-layer encryption where possible, minimising reliance on any single trusted intermediary such as a gateway.
- Educate users to recognise and avoid connecting to unknown or suspicious wireless access points.

Key Takeaways

- ✓ The I-Way is the broad conceptual infrastructure — consumer access, backbone network, service/content providers, and shared standards — that enables e-commerce traffic to flow globally.
- ✓ The Internet, built on TCP/IP, is the most important practical realisation of the I-Way today.
- ✓ WAP brought web-like services to early mobile handsets via a lightweight, layered protocol stack (WAE, WSP, WTP, WTLS, WDP) working through a WAP Gateway.
- ✓ ADSL, Wi-Fi (WLAN), WiMAX (WMAN), and cellular generations (3G/4G/5G) each address a different combination of range, speed, and mobility.
- ✓ Wireless communication's open-air nature introduces distinctive security risks — eavesdropping, rogue APs, MITM, and weak legacy encryption — that must be actively countered with strong encryption, authentication, and user awareness.

— End of Unit 2 —