📘 IoT Unit–3: Networking Technologies

RGPV Topper-Level One-Night Notes

---

1. IoT Networking Basics

Introduction

IoT networking ka matlab hai IoT devices, sensors, gateways, cloud aur user apps ko connect karna. Without networking, IoT devices data share nahi kar sakte.

Definition

IoT networking is the process of connecting IoT devices through wired or wireless communication technologies for data exchange and remote control.

Why It Is Needed

IoT networking is needed for:

- device-to-device communication
- sensor data transfer
- cloud connectivity
- remote monitoring
- automation

Easy Explanation

Sensor data collect karta hai, network us data ko gateway/cloud tak bhejta hai, aur user mobile app par result dekhta hai.

Step-by-Step Working

1. Sensor environment se data collect karta hai.
2. IoT node data process karta hai.
3. Network protocol data transfer karta hai.
4. Gateway data cloud ko bhejta hai.
5. Cloud data analyze karta hai.
6. User app output show karti hai.

Flow of Process

```
Sensor → IoT Node → Network → Gateway → Cloud → User App
```

Diagram

```
Physical Device
       ↓
Sensor
       ↓
IoT Node
       ↓
Wireless Network
       ↓
Gateway
       ↓
Cloud
       ↓
Application
```

Real-Life Analogy

Jaise WhatsApp message mobile network ke through receiver tak jata hai, waise sensor data IoT network ke through cloud tak jata hai.

Advantages

- Real-time data communication
- Remote monitoring possible
- Automation support
- Large device connectivity
- Smart decision making

Disadvantages

- Security risks
- Network failure issue
- Power consumption
- Data delay possible

Applications

- Smart homes
- Smart agriculture
- Smart city
- Industrial automation
- Healthcare monitoring

Important Keywords

Connectivity, Gateway, Protocol, Wireless Communication, Cloud, Remote Monitoring

Conclusion

IoT networking devices ko smart ecosystem me connect karta hai and data communication possible banata hai.

2. IoT Components

Introduction

IoT system different components se milkar banta hai. Har component ka separate role hota hai.

Definition

IoT components are the basic hardware and software parts required to build an IoT system.

Main Components

Component	Work
Sensor	Data collect karta hai
Actuator	Action perform karta hai
IoT Node	Data process karta hai
Gateway	Cloud se connect karta hai
Network	Data transfer karta hai
Cloud	Data store/process karta hai
Application	User interface provide karta hai

Flow

```
Sensor → Node → Gateway → Cloud → Application
```

Diagram

```
IoT System
   |
Sensor + Actuator + Network + Cloud + App
```

Example

Smart irrigation system:

- soil sensor
- controller
- gateway
- cloud
- water pump actuator

Advantages

- Organized system
- Easy automation
- Better monitoring
- Scalable design

Important Keywords

Sensor, Actuator, Gateway, Cloud, Application, Connectivity

Conclusion

IoT components together create a complete smart system for sensing, processing and action.

---

3. Functional Components of IoT

Introduction

Functional components IoT system ke working blocks hote hain. Ye batate hain ki system internally kaise kaam karta hai.

Definition

Functional components of IoT are logical modules that perform sensing, communication, processing, management, security and application functions.

Main Functional Components

Component	Function
Device Component	Sensing and actuation
Communication Component	Data transfer
Service Component	Data processing
Management Component	Device monitoring
Security Component	Data protection
Application Component	User service

Flow

```
Device → Communication → Service → Management → Application
```

Diagram

```
Functional IoT Blocks
      |
Device
Communication
Service
Management
```

```
Security
Application
```

Advantages

- Clear system structure
- Easy troubleshooting
- Better security
- Efficient management

Important Keywords

Functional Blocks, Device Management, Security, Service, Communication

Conclusion

Functional components define the logical working structure of an IoT system.

---

4. IoT Service Oriented Architecture (SOA)

Introduction

SOA ka full form **Service Oriented Architecture** hai. Isme IoT functions ko services ke form me design kiya jata hai.

Definition

IoT Service Oriented Architecture is an architecture where IoT functions are provided as independent, reusable services.

Why It Is Needed

SOA se IoT applications easily integrate, reuse and scale ho sakti hain.

Easy Explanation

SOA me har work ek service hota hai:

- sensing service
- data service
- control service
- security service

Applications in services ko use karte hain.

Layers of IoT SOA

Layer	Work
Sensing Layer	Data collect
Network Layer	Data transfer
Service Layer	Data processing
Interface Layer	User interaction

Flow

```
Sensing Layer → Network Layer → Service Layer → Interface Layer
```

Diagram

```
Interface Layer
      ↑
Service Layer
      ↑
```

```
Network Layer
      ↑
Sensing Layer
```

Real-Life Analogy

Restaurant me order service, cooking service, billing service, delivery service alag-alag hoti hain. Same SOA me IoT functions services me divide hote hain.

Advantages

- Reusable services
- Easy integration
- Scalable system
- Flexible design

Disadvantages

- Complex design
- Security management required
- Service failure affects application

Applications

- Smart city platforms
- Cloud IoT systems
- Industrial IoT
- Smart home systems

Important Keywords

SOA, Service Layer, Reusability, Interoperability, Interface Layer

Conclusion

IoT SOA system ko service-based बनाता है, जिससे IoT applications flexible and scalable बनती हैं.

---

5. IoT Challenges

Introduction

IoT systems powerful hain but unme many challenges hote hain. Security, privacy, power and interoperability major problems hain.

Definition

IoT challenges are technical and management problems faced during development, deployment and operation of IoT systems.

Main Challenges

Challenge	Easy Meaning
Security	Device/data hacking risk
Privacy	Personal data leakage
Interoperability	Different devices compatibility
Scalability	Many devices manage karna
Power Consumption	Battery issue
Connectivity	Network failure
Data Management	Huge data handling
Standardization	Common rules ki kami

Step-by-Step Problem Flow

```
Many Devices
     ↓
Huge Data
     ↓
Network Load
     ↓
Security Risk
     ↓
Management Difficulty
```

Diagram

```
IoT Challenges
   |
Security | Privacy | Power | Data | Scale | Network
```

Real-Life Analogy

Jaise large classroom me 100 students ko manage karna difficult hota hai, waise IoT me thousands devices manage karna challenging hota hai.

Advantages of Solving Challenges

- Secure system
- Better performance
- Longer device life
- Reliable communication

Disadvantages if Not Solved

- Data theft
- System failure

- Battery drain
- Poor user experience

Applications

IoT challenge handling is needed in:

- smart city
- healthcare
- banking IoT
- industrial IoT

Important Keywords

Security, Privacy, Interoperability, Scalability, Power Consumption, Data Management

Conclusion

IoT challenges must be solved to make IoT systems secure, reliable and scalable.

---

6. 6LoWPAN

Introduction

6LoWPAN ka full form **IPv6 over Low Power Wireless Personal Area Network** hai. Ye small IoT devices ko IPv6 network se connect karta hai.

Definition

6LoWPAN is a networking protocol that allows IPv6 packets to be transmitted over low-power wireless personal area networks.

Why It Is Needed

IoT devices low power aur small memory wale hote hain. IPv6 packets large hote hain. 6LoWPAN packet compression karke low-power devices ke liye communication possible banata hai.

Easy Explanation

6LoWPAN ek bridge hai between small sensor devices and IPv6 internet.

Step-by-Step Working

1. IoT device data generate karta hai.
2. IPv6 packet create hota hai.
3. 6LoWPAN packet compress karta hai.
4. Data wireless network se send hota hai.
5. Gateway data internet/cloud tak bhejta hai.

Flow

```
IoT Device → 6LoWPAN → Gateway → IPv6 Internet → Cloud
```

Diagram

```
Sensor Node
     ↓
6LoWPAN Network
     ↓
Border Router
     ↓
IPv6 Internet
```

Real-Life Analogy

Jaise large luggage ko small bag me compress karke travel karte hain, 6LoWPAN large IPv6 packet ko small packet me compress karta hai.

Advantages

- Low power communication
- IPv6 support
- Suitable for sensor networks
- Low cost

Disadvantages

- Limited bandwidth
- Complex routing
- Small packet size limitation

Applications

- Smart meters
- Home automation
- Wireless sensor networks
- Smart agriculture

Important Keywords

IPv6, Low Power, Packet Compression, WPAN, Border Router

Conclusion

6LoWPAN low-power IoT devices ko IPv6 internet se connect karne ke liye important protocol hai.

---

7. IEEE 802.15.4

Introduction

IEEE 802.15.4 low-power wireless communication standard hai. Ye ZigBee jaise protocols ka base hai.

Definition

IEEE 802.15.4 is a standard for low-rate wireless personal area networks used for low-power, low-cost IoT communication.

Why It Is Needed

IoT devices battery-powered hote hain. Unhe low power, short range aur low data rate communication chahiye. IEEE 802.15.4 ye provide karta hai.

Features

Feature	Meaning
Low Power	Battery saving
Low Cost	Cheap devices
Low Data Rate	Sensor data ke liye enough
Short Range	Personal area communication
Reliable	Stable communication

Flow

```
Sensor Node ↔ IEEE 802.15.4 Network ↔ Gateway
```

Diagram

Real-Life Analogy

Jaise small colony ke andar short-range walkie-talkie communication hota hai, waise IEEE 802.15.4 small IoT area me communication karta hai.

Advantages

- Low power
- Low cost
- Suitable for sensor networks
- Supports ZigBee

Disadvantages

- Low data rate
- Limited range
- Not suitable for video/audio heavy data

Applications

- Smart home
- Industrial sensors
- ZigBee networks
- Health monitoring devices

Important Keywords

LR-WPAN, Low Data Rate, Low Power, ZigBee Base Standard, Sensor Network

Conclusion

IEEE 802.15.4 IoT ke low-power wireless communication ke liye important standard hai.

---

8. ZigBee

Introduction

ZigBee ek low-power wireless communication protocol hai jo IoT aur sensor networks me use hota hai.

Definition

ZigBee is a low-power, low-data-rate wireless communication protocol based on IEEE 802.15.4 standard, used for IoT and sensor networks.

Why It Is Needed

IoT systems me low power aur reliable communication chahiye. ZigBee battery-powered devices ke liye suitable hai.

Easy Explanation

ZigBee Wi-Fi se slow hota hai but power kam consume karta hai. Isliye sensors ke liye best hai.

ZigBee Device Types

Type	Work
Coordinator	Network start and control karta hai
Router	Data forward karta hai
End Device	Sensor/actuator node

ZigBee Network Topologies

Topology	Meaning
Star	All devices coordinator se connected
Tree	Hierarchical structure
Mesh	Multiple paths available

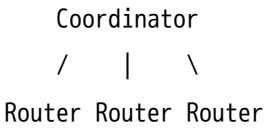
Step-by-Step Working

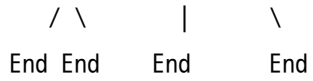
1. Coordinator network create karta hai.
2. End devices network join karte hain.
3. Sensor data generate karta hai.
4. Router data forward karta hai.
5. Coordinator/gateway data receive karta hai.

Flow

```
End Device → Router → Coordinator → Gateway → Cloud
```

Diagram





Real-Life Analogy

School me principal coordinator hai, teachers routers hain, students end devices hain.

Advantages

- Low power consumption
- Mesh networking support
- Reliable communication
- Low cost
- Good for smart homes

Disadvantages

- Low data rate
- Limited range
- Not suitable for large files

Applications

- Smart home automation
- Smart lighting
- Industrial monitoring
- Healthcare sensors

Important Keywords

Coordinator, Router, End Device, Mesh Topology, IEEE 802.15.4

Conclusion

ZigBee low-power IoT communication ke liye highly useful protocol hai, especially smart homes and sensor networks me.

---

9. RFID

Introduction

RFID ka full form **Radio Frequency Identification** hai. Ye objects ko identify and track karne ke liye radio waves use karta hai.

Definition

RFID is a wireless identification technology that uses radio waves to read data stored in RFID tags.

Why It Is Needed

RFID fast and automatic identification ke liye use hota hai. Barcode ki tarah line-of-sight zaroori nahi hoti.

Components

Component	Work
RFID Tag	Object par attached hota hai
RFID Reader	Tag data read karta hai
Antenna	Radio signal transmit/receive
Database	Object data store karta hai

Step-by-Step Working

1. RFID reader radio signal send karta hai.
2. RFID tag signal receive karta hai.

3. Tag apna stored ID reader ko send karta hai.
4. Reader data database ko bhejta hai.
5. Object identify hota hai.

Flow

```
Reader → Radio Signal → Tag → ID Data → Reader → Database
```

Diagram

```
RFID Tag ↔ RFID Reader ↔ Database
```

Real-Life Analogy

RFID school ID card jaisa hai. Card scan hote hi student ki information system me aa jati hai.

Advantages

- Fast identification
- No line-of-sight needed
- Multiple tags scan possible
- Automatic tracking

Disadvantages

- Security risk
- Cost higher than barcode
- Signal interference possible

Applications

- Inventory management
- Library systems
- Toll collection
- Attendance systems
- Supply chain tracking

Important Keywords

RFID Tag, RFID Reader, Radio Waves, Identification, Tracking

Conclusion

RFID IoT me objects ko identify and track karne ke liye powerful wireless technology hai.

---

10. NFC

Introduction

NFC ka full form **Near Field Communication** hai. Ye very short-range wireless communication technology hai.

Definition

NFC is a short-range wireless communication technology that allows two devices to exchange data when placed very close to each other.

Why It Is Needed

Secure and quick data exchange ke liye NFC useful hai, especially payments and smart cards me.

Easy Explanation

NFC tab kaam karta hai jab two devices very close hote hain, usually 10 cm ke andar.

Step-by-Step Working

1. NFC reader electromagnetic field create karta hai.
2. NFC tag/device close aata hai.
3. Tag activate hota hai.
4. Data exchange hota hai.
5. Transaction/operation complete hota hai.

Flow

```
NFC Device 1 ↔ Very Short Range ↔ NFC Device 2
```

Diagram

```
Mobile Phone ↔ NFC Tag/Card
```

Real-Life Analogy

Tap-to-pay card NFC ka example hai. Card machine ke close laate hi payment process hota hai.

Advantages

- Secure due to short range
- Fast connection

- Easy to use
- No pairing required

Disadvantages

- Very short range
- Low data speed
- Not suitable for long-distance communication

Applications

- Contactless payment
- Smart cards
- Access control
- Ticketing systems

Important Keywords

Near Field, Contactless, Short Range, Tap-to-Pay, Smart Card

Conclusion

NFC short-range secure communication ke liye useful hai, especially payment and identification systems me.

---

11. Bluetooth

Introduction

Bluetooth ek short-range wireless communication technology hai. Ye nearby devices ko connect karta hai.

Definition

Bluetooth is a short-range wireless communication technology used for exchanging data between nearby devices.

Why It Is Needed

Small distance me wireless connectivity ke liye Bluetooth use hota hai.

Easy Explanation

Bluetooth devices pairing karke data exchange karte hain.

Step-by-Step Working

1. Device Bluetooth ON karta hai.
2. Nearby device discover hota hai.
3. Pairing process hota hai.
4. Connection establish hota hai.
5. Data exchange hota hai.

Flow

```
Device Discovery → Pairing → Connection → Data Transfer
```

Diagram

```
Smartphone ↔ Bluetooth Earbuds
```

Real-Life Analogy

Wireless earphones phone se Bluetooth ke through connect hote hain.

Advantages

- Wireless
- Low cost
- Low power
- Easy connection

Disadvantages

- Limited range
- Lower speed than Wi-Fi
- Security risk if pairing unsafe

Applications

- Wireless headphones
- Smart watches
- Health devices
- IoT home devices

Important Keywords

Pairing, Short Range, Bluetooth Low Energy, Wireless Communication

Conclusion

Bluetooth short-range IoT communication ke liye simple and popular technology hai.

---

12. MQTT / CoAP Related Networking

Introduction

MQTT and CoAP IoT communication protocols hain. Ye lightweight protocols hain jo low-power devices ke liye useful hote hain.

Definition

MQTT is a lightweight publish-subscribe messaging protocol used for IoT communication.
CoAP is a lightweight web transfer protocol designed for constrained IoT devices.

Why It Is Needed

IoT devices small memory and low power wale hote hain. Heavy protocols unke liye suitable nahi hote. MQTT and CoAP lightweight communication provide karte hain.

MQTT Working

```
Publisher → Broker → Subscriber
```

Example: Temperature sensor data publish karta hai. Mobile app subscriber hoti hai.

CoAP Working

```
Client → Request → Server
Server → Response → Client
```

CoAP REST model jaisa kaam karta hai.

Comparison Table

Basis	MQTT	CoAP
Model	Publish-subscribe	Request-response
Transport	TCP	UDP
Best For	Continuous messaging	Resource-constrained web devices
Middle Component	Broker required	Broker not required
Example	Sensor updates	Smart bulb control

Which is Better and Why?

- MQTT better hai continuous sensor data updates ke liye.
- CoAP better hai constrained devices ke request-response communication ke liye.

  Use case ke according dono important hain.

Diagram

```
MQTT:
Sensor → Broker → Mobile App

CoAP:
Client ↔ Server
```

Advantages

MQTT

- Lightweight
- Reliable messaging
- Good for remote monitoring

CoAP

- Lightweight
- Web-like communication
- Low overhead

Disadvantages

MQTT

- Broker dependency

CoAP

- UDP reliability issue

Applications

- Smart home
- Sensor monitoring
- Industrial IoT
- Smart agriculture

Important Keywords

MQTT, CoAP, Publish-Subscribe, Broker, Request-Response, Lightweight Protocol

Conclusion

MQTT and CoAP are important lightweight IoT protocols used for efficient communication in constrained networks.

---

13. Wireless Sensor Network (WSN)

Introduction

WSN wireless sensor nodes ka network hota hai. Ye environment data collect karke base station ko send karta hai.

Definition

Wireless Sensor Network is a network of spatially distributed sensor nodes that monitor physical conditions and communicate wirelessly.

Why It Is Needed

Remote areas me wired network possible nahi hota. WSN wireless sensing and monitoring provide karta hai.

Components

Component	Work
Sensor Node	Data collect karta hai
Sink/Base Station	Data receive karta hai
Gateway	Cloud/internet se connect karta hai
Wireless Link	Data transfer karta hai

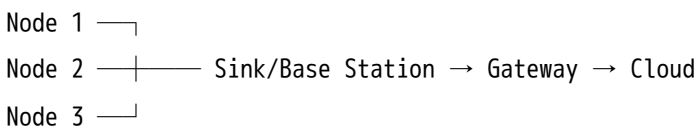
Step-by-Step Working

1. Sensor nodes environment monitor karte hain.
2. Data nearby node/sink ko send hota hai.
3. Sink/base station data collect karta hai.
4. Data processing/application me use hota hai.

Flow

```
Sensor Nodes → Sink Node → Gateway → Cloud
```

Diagram



Real-Life Analogy

Classroom me students information collect karke monitor ko dete hain, monitor teacher ko report karta hai.

Advantages

- Remote monitoring
- Wireless deployment
- Scalable
- Useful in dangerous areas

Disadvantages

- Battery limitation
- Security issues
- Limited processing power
- Network failure risk

Applications

- Forest fire detection

- Smart agriculture
- Military surveillance
- Health monitoring
- Environmental monitoring

Important Keywords

Sensor Node, Sink Node, Base Station, Wireless Communication, Remote Monitoring

Conclusion

WSN IoT ka important part hai jo wireless sensors ke through real-time monitoring possible banata hai.

🔥 Comparison Table: ZigBee vs Bluetooth vs NFC vs RFID

Basis	ZigBee	Bluetooth	NFC	RFID
Range	Medium	Short	Very short	Short to medium
Power	Very low	Low	Very low	Low
Data Rate	Low	Medium	Low	Low
Main Use	Sensor network	Device connection	Payment/access	Identification
Example	Smart home sensors	Earbuds	Tap payment	ID card

🔥 Comparison Table: 6LoWPAN vs ZigBee

Basis	6LoWPAN	ZigBee
Full Form	IPv6 over Low Power WPAN	ZigBee protocol
Internet Support	Direct IPv6 support	Needs gateway
Base Standard	IEEE 802.15.4	IEEE 802.15.4

Basis	6LoWPAN	ZigBee
Use	IP-based IoT	Low-power sensor networks
Advantage	Internet integration	Mesh networking

🔥 Most Important 7-Mark Questions

1. Explain ZigBee and its types.
2. Explain RFID working principle and applications.
3. Explain 6LoWPAN.
4. Explain IEEE 802.15.4.
5. Explain NFC.
6. Explain Bluetooth.
7. Explain Wireless Sensor Network.
8. Explain IoT challenges.
9. Explain MQTT and CoAP.
10. Explain IoT SOA.

⭐ Most Important 14-Mark Questions

1. Explain ZigBee architecture, device types and network topologies.
2. Explain RFID features, working principle and applications.
3. Explain WSN architecture and applications.
4. Explain IoT networking technologies: 6LoWPAN, IEEE 802.15.4, ZigBee, RFID, NFC and Bluetooth.
5. Explain MQTT and CoAP with comparison.
6. Explain IoT functional components and service-oriented architecture.

🎯 PYQ-Based Expected Questions

Very High Probability

✅ ZigBee
✅ RFID
✅ MQTT/CoAP related networking
✅ WSN
✅ IEEE 802.15.4

High Probability

✅ NFC
✅ Bluetooth
✅ IoT Challenges
✅ 6LoWPAN

Medium Probability

✅ SOA
✅ Functional Components
✅ IoT Networking Basics

⚡ One-Night Revision Notes

Topic	Quick Revision
ZigBee	Low-power mesh IoT protocol
IEEE 802.15.4	Base standard for low-rate WPAN
6LoWPAN	IPv6 for low-power devices
RFID	Radio-based identification
NFC	Very short-range communication
Bluetooth	Short-range wireless pairing
MQTT	Publish-subscribe protocol
CoAP	Request-response lightweight protocol
WSN	Network of wireless sensor nodes
SOA	Service-based architecture

📌 Smart Study Plan

2-Hour Plan

Time	Topic
20 min	ZigBee
20 min	RFID
15 min	6LoWPAN
15 min	IEEE 802.15.4
15 min	WSN
15 min	MQTT/CoAP
10 min	NFC + Bluetooth
10 min	SOA + Challenges

5-Hour Plan

Time	Topic
1 hour	ZigBee + IEEE 802.15.4
1 hour	RFID + NFC + Bluetooth
1 hour	6LoWPAN + MQTT/CoAP
1 hour	WSN + applications
1 hour	SOA + components + challenges

🧠 Memory Tricks

ZigBee Devices

CRE

- C = Coordinator

- R = Router
- E = End Device

RFID Components

TRD

- T = Tag
- R = Reader
- D = Database

IoT Challenges

SPCID

- S = Security
- P = Privacy
- C = Connectivity
- I = Interoperability
- D = Data Management

Networking Technologies

ZRBNC

- Z = ZigBee
- R = RFID
- B = Bluetooth
- N = NFC
- C = CoAP

🚀 Topper Answer Writing Tips

For 7 marks:

```
Definition
↓
Working
↓
Diagram
↓
Advantages
↓
Applications
↓
Conclusion
```

For 14 marks:

```
Introduction
↓
Definition
↓
Architecture / Components
↓
Detailed Working
↓
Diagram
↓
Comparison Table
↓
Applications
↓
Conclusion
```

Keywords to Underline

ZigBee, Coordinator, Router, End Device, RFID Tag, RFID Reader, NFC, Bluetooth, 6LoWPAN, IEEE 802.15.4, MQTT, CoAP, WSN, SOA

Final tip: सबसे पहले **ZigBee + RFID + WSN + 6LoWPAN + IEEE 802.15.4** prepare करो. Unit-3 में यही सबसे scoring topics हैं.