Understanding Cisco Wireless Foundations (WLFNDU)

Course Duration: 40 Hours **Course code: WLFNDU**

1. Course Overview

This course provides foundational knowledge of Cisco wireless technologies and prepares learners to understand, configure, and troubleshoot basic wireless networks. Participants will gain insight into wireless LAN components, RF fundamentals, security, and basic troubleshooting practices within Cisco WLAN environments.

2. What you'll learn?

By the end of this course, learners should be able to:

- Describe wireless network concepts and components
- Explain RF fundamentals and their impact on WLAN performance
- Understand Cisco Wireless LAN architecture and deployment models
- Configure basic WLAN services and AP settings
- Implement foundational wireless security measures
- Use basic monitoring and troubleshooting techniques

3. Target Audience

- Network engineers and administrators new to wireless technologies
- IT professionals supporting Cisco WLAN deployments
- Technical staff preparing for advanced wireless courses
- Anyone seeking foundational knowledge of Cisco wireless networks

4. Pre-Requisites

Familiarity with:

- Networking fundamentals (TCP/IP, VLANs, switching)
- Basic routing concepts
- General understanding of IT infrastructure

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

5. Course content

Module 1: Course Introduction

- Introduction
- Course contents

Module 2: Wireless Networking Fundamentals

- WLAN components and architecture
- Types of wireless networks (enterprise, campus, remote)
- Wireless standards (802.11a/b/g/n/ac/ax)

Module 3: RF Fundamentals

- Understanding RF spectrum
- Channels, frequency bands, and interference
- Signal propagation, attenuation, and coverage

Module 4: Cisco Wireless LAN Architecture

- Cisco Unified Wireless Network (CUWN) overview
- Access Points and Controllers
- Deployment models: centralized vs. distributed
- Cisco DNA Center introduction

Module 5: Wireless Client Devices

- Client types and compatibility
- Association and authentication process
- Roaming concepts and considerations

Module 6: Wireless Security Fundamentals

- Security threats in WLAN
- Authentication and encryption (WPA2, WPA3, 802.1X)
- Rogue AP detection and mitigation

Module 7: Basic WLAN Configuration

- Configuring SSIDs and VLAN mapping
- AP and controller basic configuration
- Wireless client connectivity

Module 8: WLAN Monitoring and Troubleshooting

- Monitoring WLAN performance
- Identifying RF interference issues
- Basic troubleshooting tools and techniques

Module 9: Introduction to Wireless Policies and QoS

- Traffic prioritization and QoS concepts
- WLAN policy basics
- Band steering and client load balancing

Module 10: Wireless Best Practices

- Site survey basics
- Coverage planning and AP placement
- Security and operational best practices

Module 11: Case Studies and Examples

- Simple enterprise WLAN scenarios
- Lessons learned from real-world deployments
- Applying foundational concepts in practice

Module 12: Course Wrap-Up

- Summary of key concepts
- Q&A session
- References and next steps for advanced courses