DCT Certified Network Infrastructure Professional

Duration: 5 Days

Course Code: DCT-DCNIP

About this course:

Today's Network Infrastructure for smart buildings starts with the foundation of copper and fiber cabling supported by Networking and wireless equipment to support POE devices on LAN and IoT devices. The DCT Certified Network Infrastructure professional (CNIP) is a 5 days intensive practical course with the aim to develop knowledge and skills to design and implement complex projects. The course covers Network fundamentals , Networking standards , Wireless , Security , unified communications , Copper Systems and Fiber systems . The course covers in-depth knowledge of testing on copper and fiber systems based on international standards and cable testing giving warranty on passive cabling systems. On completion of the course the learner will be able to gain confidence to design , scope , document , implement and install and deliver complex infrastructure systems with focus on quality , timescales within agreed budget.

Course outline:

Networking Concepts

- Explain the purposes and uses of ports and protocols.
- Explain devices, applications, protocols and services at their appropriate OSI layers.
- Explain the concepts and characteristics of routing and switching.
- Given a scenario, configure the appropriate IP addressing components.
- Compare and contrast the characteristics of network topologies, types and technologies.
- Given a scenario, implement the appropriate wireless technologies and configurations.
- Summarize cloud concepts and their purposes.
- Explain the functions of network services.

Infrastructure

- Given a scenario, deploy the appropriate cabling solution.
- Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them.
- Explain the purposes and use cases for advanced networking devices.
- Explain the purposes of virtualization and network storage technologies.
- Compare and contrast WAN technologies.

Horizontal Cabling

- Given a scenario, use appropriate documentation and diagrams to manage the network.
- Compare and contrast business continuity and disaster recovery concepts.
- Explain common scanning, monitoring and patching processes and summarize their expected outputs.
- Given a scenario, use remote access methods.
- Identify policies and best practices.

Network Security

- Summarize the purposes of physical security devices.
- Explain authentication and access controls.
- Given a scenario, secure a basic wireless network.
- Summarize common networking attacks.
- Given a scenario, implement network device hardening.
- Explain common mitigation techniques and their purposes.

Network Troubleshooting and Tools

- Explain the network troubleshooting methodology
- Given a scenario, use the appropriate tool
- Given a scenario, troubleshoot common wired connectivity and performance issues.
- Given a scenario, troubleshoot common wireless connectivity and performance issues.
- Given a scenario, troubleshoot common network service issues.