



Managing Industrial Networks with Cisco Networking Technologies (200-401)

Exam Description: The IMINS 200-401 Managing Industrial Networks with Cisco Networking Technologies exam is a 75-minute, 60–70 question assessment within the Cisco Internet of Things Specialist certification. This exam tests a candidate's knowledge of the OSI layers of IP networks, as well as networking devices like routers and switches, and cabling approaches; specific industrial devices such as drives, PLCs, sensors, and substation equipment; relevant industrial standards and models such as TIA, the Purdue model, and environmental standards; and various safety protocols important in an industrial zone. Candidates can prepare for this exam by taking the Managing Industrial Networks with Cisco Networking Technologies course.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

- 15%** **1.0 Install, Replace, and/or Remove an End-Device**
 - 1.1 Demonstrate knowledge of different industrial end-point devices and the interconnections for those devices to perform appropriately in an industrial setting to incorporate elements of bandwidth, real-time, precision, etc.
 - 1.2 Given a config script for a topology determine the appropriate location for the installation of the industrial ruggedized end-point device and how that device will interact with other elements.
 - 1.3 Ensure proper industrial network operation of a given end-device following replacement by verifying that industrial ruggedized elements (ports, IP address, connectivity, subnet mask, default gateway) are appropriately configured/connected.
 - 1.4 Demonstrate an understanding of safe physical installation of various industrial ruggedized end-devices within an industrial setting following a terminal block diagram.

- 23%** **2.0 Install, Replace, and/or Remove an Infrastructure Device**
 - 2.1 Demonstrate a knowledge of how different industrial application/network protocols operate within the network topology (Ethernet/IP, 61850, etc.)
 - 2.2 Demonstrate familiarity with basic CLI/GUI configuration within an industrial network by accessing, configuring, saving, validating (ports, IP address, connectivity, subnet mask, default gateway) and exiting a network device.
 - 2.3 Demonstrate understanding of safe physical installation of various industrial ruggedized network devices within an industrial setting, (e.g. following a schematic such as a terminal block diagram, and the interdependencies of the network infrastructure devices.)
 - 2.4 Demonstrate knowledge of different industrial network infrastructure devices, their places in the industrial network, and the networking/device characteristics such as QoS, precise timing, industrial topologies, network resiliency, ruggedization, bandwidth, etc.
 - 2.5 Illustrate understanding of the interconnections for the full network within a validation of the entire industrial network connectivity and that it is aligned with the provided design diagram (correct number of devices and/or IP addresses, cables are properly labelled and connected to the proper places, usage of appropriate icons) to include ensuring that configuration files are up to date and available.
 - 2.6 Illustrate an understanding of the safety and security risks (company or industry, e.g. Purdue model) for a given industrial infrastructure device and apply the appropriate steps to secure it (e.g. are unused ports turned off, telnet versus SSH, https versus http, network segmentation.)

10%	3.0	Install, Replace, and/or Remove Cables (network and/or power)
	3.1	Demonstrate the selection of cable channel for an industrial application with appropriate cable and connectors, for example two-pair, four-pair cable, high-flex, high- EMI, unshielded, fiber, and copper.
	3.2	Demonstrate safe and secure installation, identification, and documentation best practices for various industrial environments including grounding, bonding, shielding, etc. (for example: TIA1005, TIA568c.0, EN10174, TIA606b, and NEC article 800.)
	3.3	Identify the steps and tools for validating the newly installed cabling and connectors (for example: TIA568c.2.)
35%	4.0	Troubleshooting
	4.1	Layer 1
	4.1.a	Identify cable or device issues by visual inspection, test tools, and examining traffic statistics via system logs and/or end devices UIs.
	4.1.b	Characterize the symptoms associated with a duplex mismatch situation.
	4.2	Layer 2
	4.2.a	Given a scenario in an industrial setting, troubleshoot a switch port by reviewing the UI, configuration, link lights, and/or looking at counters or packet capture (e.g. multicast, QoS.)
	4.2.b	Given network symptoms identify the likely errors and the root causes of those errors (e.g. baud rate, network loops, spanning tree.)
	4.3	Layer 3
	4.3.a	Given a scenario in an industrial setting, troubleshoot a networking device by reviewing the UI, configuration, addressing/subnet mask, link lights, and/or looking at counters or packet capture (e.g. routing protocol, QoS, duplicate IP.)
	4.3.b	Determine if there is layer 3 connectivity using common tools (e.g. trace route, ping, etc.)
	4.4	End-to-End
	4.4.a	Determine if there is application connectivity and appropriate industrial performance using common tools (e.g. trace route, ping, telnet, etc.)
	4.5	Relevant Networking Issues
	4.5.a	Identify and collect relevant troubleshooting information for issue reporting/escalation/duplication.
	4.5.b	Demonstrate appropriate knowledge to proactively identify cyber and physical security incidents.
	4.5.c	Demonstrate an understanding of secure, safe, and non-disruptive methods during industrial network monitoring and diagnosis.
17%	5.0	Maintain Appropriate End-Devices and Industrial Network Infrastructure Devices
	5.1	Given a scenario, ensure reliable back-ups of current configuration are being made.
	5.2	Given a scenario, verify that the appropriate firmware is loaded to support the system.
	5.3	Demonstrate an understanding of the importance of maintaining updated firmware to minimize security holes.
	5.4	Demonstrate an understanding of appropriate techniques to upload software to a Cisco IOS networking device.

- 5.5 Provided a deployed asset inventory database illustrate an understanding of appropriate methods for updating and/or maintaining the database (hardware, operating system and patch level, which people have access to different systems.)
- 5.6 Demonstrate an understanding of the conditions that cause deterioration of equipment (cables, devices, etc.) as related to industrial environments.
- 5.7 As part of the change management process identify the relevant documentation artifacts to be maintained for all stakeholders.