Managing Industrial Networks for Manufacturing with Cisco Technologies (200-601)

Exam Description: The Managing Industrial Networks for Manufacturing with Cisco Technologies (IMINS2) certification exam (200-601) is a 90 minute, 65 – 75 question assessment. This exam tests concepts and technology commonly found in the automated manufacturing environment. This exam tests candidates on the Common Industrial Protocol (CIP) and ProfiNET industrial protocols and the underlying support network infrastructure design to maximize efficiency within Industrial Ethernet (IE).

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.

20%	**1.0**	**IP Networking**
	1.1	Describe the difference between enterprise environments and industrial environments
	1.2	Describe the components for making the data flow highly available and predictable in an industrial environment (QoS, IP addressing, protocol, and hardware resiliency)
	1.3	Interpret and diagnose problems that are related to QoS
	1.4	Describe the differences between redundancy and resiliency requirements / approaches between the enterprise and the plant floor
	1.5	Differentiate the capabilities of switch types
	1.6	Describe the life cycle of a multicast group
	1.7	Describe and configure the operation and use cases for NAT
	1.8	Describe and configure the operation and use cases for static routing
	1.9	Describe and configure VLAN trunking to a virtual switch
	1.10	Describe and configure Layer 2 resiliency protocols (Spanning Tree, REP, Flex Links, and Etherchannels)
	1.11	Configure switch ports (macros, threshold alarms)
19%	**2.0**	**Common Industrial Protocol (CIP) Knowledge and Configuration**
	2.1	Explain the CIP connection establishment process
	2.2	Explain producer/consumer models and implicit/explicit message models
	2.3	Recognize communication abilities and capacities in different hardware/hardware generations (revisions)
	2.4	Identify and describe the technologies that enable CIP Motion and CIP Safety
	2.5	Identify the applicability, limitations, and components of a DLR implementation
	2.6	Implement multicast features for CIP within a LAN
	2.7	Optimize RPI on a CIP connection given a set of parameters
	2.8	Enable and configure IEEE 1588 PTP at the system level
	2.9	Configure the Stratix using the Add On Profile (AOP) in Studio 5000

19% 3.0 ProfiNET Knowledge and Configuration

3.1 Describe the differences in ProfiNET support between Cisco catalyst and Cisco Industrial Ethernet (IE) switches
- 3.1.a Support for VLAN 0
- 3.1.b Support for ProfiNET LLDP
- 3.1.c Support for GSDs (integration into SIMATIC STEP 7)

3.2 Describe the operation and purpose of ProfiSAFE

3.3 Describe the three basic ProfiNET devices and conformance classes

3.4 Describe the ProfiNET application classes and communication channels

3.5 Describe DCP and how it can be used for IP addressing of devices and configuration pushes

3.6 Describe ring network requirements for ProfiNET

3.7 Enable ProfiNET on the switch

3.8 Enable Layer 2 QoS to ensure ProfiNET is prioritized

3.9 Integrate the Cisco IE Switch in SIMATIC STEP 7

3.10 Configure and monitor ProfiNET alarm profiles on IE switches

12% 4.0 Security

4.1 Describe the defense in-depth approach to securing the industrial zone

4.2 Identify how a security component (hardware/software) applies to a network device to meet the network security definition of defense in depth

4.3 Describe network device hardening

4.4 Describe the concept and mechanisms of implementing logical segmentation

4.5 Identify possible options to control traffic between zones (ACLs, firewalls, VLANs)

10% 5.0 Wireless

5.1 Describe the differences between 802.11a/b/g/n/ac

5.2 Describe the components that you need to build multiple wireless networks on a single access point

5.3 Describe the difference between autonomous and controller-based access points and wireless workgroup bridges

5.4 Demonstrate a typical switchport configuration for autonomous and controller-based access points

5.5 Describe the limitations of using a workgroup bridge with a control communication

20% 6.0 Troubleshooting

6.1 Troubleshoot advanced Layer 1 problems such as mechanical deterioration, electromagnetic noise issues, and infrastructure mismatches

6.2 Troubleshoot VLAN trunking
6.3 Troubleshoot an error disabled port
6.4 Troubleshoot basic spanning tree port state and root priority problems
6.5 Troubleshoot Layer 3 problems by inspecting route tables and NAT tables
6.6 Troubleshoot Layer 3 problems in a VRF-lite enabled environment
6.7 Demonstrate the ability to find the location of a device within a multi-switch network given an IP address
6.8 Identify methods for troubleshooting a communication problem in a CIP environment
6.9 Troubleshoot CIP using an Ethernet/IP browse tool, command line, and a web browser
6.10 Troubleshoot device communications performance
6.11 Identify the source of cable and device faults in a DLR
6.12 Identify methods for troubleshooting a communication problem in a ProfiNET environment
6.13 Troubleshoot ProfiNET using SIMATIC STEP 7 to view network topology, use the switch command line