Managing Industrial Networks for Manufacturing with Cisco Technologies

(200-601)

Exam Description: The exam Managing Industrial Networks for Manufacturing with Cisco Technologies (CCNA 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.

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
  - 1.1.a Enterprise priorities
    - 1.1.a.1 Confidentiality
    - 1.1.a.2 Integrity
    - 1.1.a.3 Availability
  - 1.1.b Industrial Priorities
    - 1.1.b.1 Availability
    - 1.1.b.2 Integrity
    - 1.1.b.3 Confidentiality

- 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)
  - 1.2.a Understand which data flows must be prioritized in an industrial environment
  - 1.2.b What are we protecting
  - 1.2.c What technologies enable prioritization (threshold alarms, QoS and IGMP multicast controls)

- 1.3 Interpret and diagnose problems that are related to QoS
  - 1.3.a How do you know that the QoS policy is doing its job
  - 1.3.b Why and when are packets being dropped

- 1.4 Describe the differences between redundancy and resiliency requirements / approaches between the Enterprise and the plant floor
  - 1.4.a First hop redundancy and resiliency, stacking and HSRP
  - 1.4.b Plant floor focuses on availability of production more than availability of the network

1.4.c Multiple lines, multiple end points vs highly resilient uplinks to the network, graceful degradation

1.5 Differentiate the capabilities of switch types
- 1.5.a Classic Layer 2, classic Layer 3, managed, unmanaged, industrial
- 1.5.b Some Layer 2 switches have Layer 3 switching attributes

1.6 Describe the life cycle of a multicast group
- 1.6.a How does the joining process work
- 1.6.b How does multicast work (emphasis on LAN)
- 1.6.c What is multicast IGMP doing
- 1.6.d What is the relationship between IP addressing and MAC addressing

1.7 Describe and configure the operation and use cases for NAT
- 1.7.a What scenarios use NAT
- 1.7.b What are the strengths and weaknesses of NAT

1.8 Describe and configure the operation for static routing
- 1.8.a What scenarios use static routing
- 1.8.b What are the strengths and weaknesses of static routing

1.9 Describe and configure VLAN trunking to a virtual switch
- 1.9.a Describe the multiple ways to do server virtualization, link virtual servers together

1.10 Describe and configure Layer 2 resiliency protocols (Spanning Tree, REP, Flex Links, and Etherchannels)
- 1.10.a Limitations of Etherchannels
- 1.10.b Limitations of spanning tree, REP, Flex Links, Etherchannels
- 1.10.c Spanning tree portfast, priorities, guards

1.11 Configure switch ports (macros, threshold alarms)
- 1.11.a Threshold limits being exceeded get an alarm
- 1.11.b Understand the likely causes of the alarm
  - 1.11.b.1 Too many connections

19% 2.0 CIP

2.1 Explain the CIP connection establishment process
- 2.1.a What are TCP and UDP are used for

2.2 Explain producer/consumer models and implicit/explicit message models
- 2.2.a Implicit is UDP multicast or unicast
- 2.2.b Explicit is TCP
- 2.2.c CIP connected or CIP unconnected

2.3 Recognize communication abilities and capacities in different hardware/hardware generations (revisions)
- 2.3.a End point I/O and control, thresholds, PPS, multicast vs unicast

2.3.b Given a table be able to interpret throughput vs thresholds (setting alarms)
2.3.c Examine macros and understand implications
2.3.d Understand limitations of a CIP environment

2.4 Identify and describe the technologies that enable CIP Motion and CIP Safety
2.4.a PTP – best master clock algorithm
2.4.b PTP, multicast, QoS, full duplex
2.4.c QoS – what are ODVA recommended QoS markings and queue mappings for an industrial automation network
2.4.d Documents – ODVA, CPwE
2.4.e Describe the communication technique black channel principle

2.5 Identify the applicability, limitations, and components of a DLR implementation
2.5.a Know the functionality of the DLR supervisor
2.5.b Know when to use ETAP, fast convergence time

2.6 Implement multicast features for CIP within a LAN
2.6.a Setting up IGMP using templates (snooping, query per VLAN)
2.6.b Alarm threshold use case

2.7 Optimize RPI on a CIP connection given a set of parameters
2.7.a What to set it to (limitations of the device – e.g. switches, controllers, I/O end points)

2.8 Enable and configure IEEE 1588 PTP at the system level
2.8.a Enabling boundary clocks
2.8.b Selecting a grand master
2.8.c Enabling transparent clocks
2.8.d Checking clock synchronization
2.8.e Priority setting

2.9 Configure the Stratix using the Add On Profile (AOP) in Studio 5000

19% 3.0 ProfiNET

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
3.3.a Controller, Supervisor and I/O device
3.3.b Class A, B, C Cisco IE switches meet class A and B requirements

3.4 Describe the ProfiNET application classes and communication channels
3.4.a ProfiNET CBA and ProfiNET I/O

3.4.b ProfiNET NRT, RT and IRT
3.4.c Cyclic I/O, Acyclic I/O, multicast I/O

3.5 Describe DHCP and how it can be used for IP addressing of devices and configuration pushes
3.5.a Describe how DHCP can be used for auto configuration

3.6 Describe ring network requirements for ProfiNET
3.6.a Understand the three redundancy classes
3.6.a.1 Class 1
3.6.a.2 Class 2
3.6.a.3 Class 3
3.6.b Discuss MRP and REP and their differences

3.7 Enable ProfiNET on the switch
3.7.a Turn on ProfiNET and define the VLAN

3.8 Enable Layer 2 QoS to ensure ProfiNET is prioritized

3.9 Integrate the Cisco Industrial Ethernet Switch in SIMATIC STEP 7
3.9.a Copy the GSD file off the Cisco Industrial Ethernet Switch and load into SIMATIC STEP 7
3.9.b Describe the purpose of a GSD file and understand how to locate it on a Cisco switch
3.9.c Check that the topology has been discovered on SIMATIC STEP 7
3.9.c.1 Show LLDP and ProfiNET LLDP information on switch

3.9.d Use and monitor ProfiNET LLDP on the switch (Cisco Industrial Ethernet Switch)
3.9.e ProfiNET extensions are NOT supported on non-industrial switches
3.9.f Topology discovery in SIMATIC STEP 7 and also for auto-configuration
3.9.g Use show commands to see if ProfiNET is working properly
3.9g.1 Show LLDP and ProfiNET LLDP information on switch
3.9.g.2 Show ProfiNET status

3.10 Configure and monitor ProfiNET alarm profiles on IE switches
3.10.a Show monitoring in SIMATIC STEP 7
3.10.b Create a global alarm profile, apply it to an interface, pull a cable and see if alarm appears on SIMATIC

12% 4.0 Security

4.1 Describe the defense in-depth approach to securing the industrial zone
4.1.a Identify the 6 layer model – device hardening, application security, computer hardening, network security, physical security, policies/procedures/awareness

4.2 Identify how a security component (hardware/software) applies to a network device to meet the network security definition of defense in depth
4.2.a AAA, perimeter protection, intrusion detection/prevention, end point protection

4.2.a.1 Fit the previous examples into the right layer
4.2.b.1 Where would you deploy intrusion protection
4.2.c.1 What policies would apply

4.3 Describe network device hardening
4.3.a SSH, control plane policing, restricting physical access, authentication

4.4 Describe the concept and mechanisms of implementing logical segmentation
4.4.a ACLs, firewalls, VLANs, industrial DMZ, VRF

4.5 Identify possible options to control traffic between zones (ACLs, firewalls, VLANs)
4.5.a Industrial zone and the enterprise zone and between the cell area zone and the industrial zone
4.5.b OPC, firewall, VLANs, remote access
4.5.b.1 Remote access question, data movement question

4.5.c Properly apply access control lists to routers and switches to allow or limit specific traffic
4.5.d Show ways to pass/limit data between cells

10% 5.0 Wireless

5.1 Describe the differences between 802.11a/b/g/n/ac
5.1.a Speeds, frequencies, number of non-overlapping channels, RF interference

5.2 Describe the components that you need to build multiple wireless networks on a single access point
5.2.a SSIDs, SSID map to VLANs; RF spectrum
5.2.b Describe why you would have multiple SSIDs
5.2.c WPA, WEP, TKIP, AES

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
5.5.a Take an autonomous AP and a workgroup AP configuration file and build a workgroup bridge
5.5.b Why and when would you use a workgroup bridge
5.5.c Performance limit recommendations: 20 total wireless nodes (per AP) – from testing with no more than 19 wired clients (per WGB); 2200 pps in the wireless channel (less with interference); 20% BW reservation for HMI + maintenance traffic (must include non-CIP packets)

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
- 6.2.a Native VLAN mismatch, encapsulation types, allowed VLAN list
- 6.2.b Enable network card to see VLAN tags for packet capture

6.3 Troubleshoot an error disabled port
- 6.3.a MAC address change/port security, UDLD, root guard, BPDU

6.4 Troubleshoot basic spanning tree port state and root priority problems
- 6.4.a Listening, learning, blocking, root bridge priority
- 6.4.b Identify broadcast storm

6.5 Troubleshoot Layer 3 problems by inspecting route tables and NAT tables
- 6.5.a Access list problems where something is not communicating – where is the access list misconfigured? NAT device is not communicating, incorrectly configured static routes
- 6.5.b Look at diagnostic screen and identify what is happening on the network
- 6.5.c Show a diagnostic readout and identify which diagnostic parameter is indicating an error

6.6 Troubleshoot Layer 3 problems in a VRF-lite enabled environment
- 6.6.a Recognize when VRF is active on a device and be able to understand the various differences (commands, tables)
- 6.6.b Show ARP tables from two different VRFs

6.7 Demonstrate the ability to find the location of a device within a multi-switch network given an IP address
- 6.7.a Ping it, traceroute it, check ARP, get its MAC address, check CAM, which port is it on

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
- 6.9.a Identify that appropriate multicast controls are active in a CIP environment
- 6.9.b Prove that multicast is enabled and functioning properly (is switch configured properly, is there an IGMP query)
- 6.9.c Show an IGMP snoop table
- 6.9.d Show that CIP multicast addresses are listed in the snooping table

6.10 Troubleshoot device communications performance
- 6.10.a Use a UI and network tools to identify threshold limits – Wireshark, switch alarm thresholds, RPI, port counters, MAC address table inspection
- 6.10.b Identify which device is the source of the issue and the resolution. (shut the offending port down, change software)
- 6.10.c Number of connections
- 6.10.d Validate that a CIP connection is active
- 6.10.e Difference between a CIP connection and a TCP connection

6.10.f Look at Wireshark, physical integrity, network integrity, collect traces, spanning tree, using VLAN, using remote VLAN

6.10.g Show a simple diagram and know where and why they are collecting a trace from a particular place in the network

6.10.h When you collect a trace, why do you not see the startup of a CIP connection (packet number, sequence number, power down, recycle cards)

6.10.i Interpret a piece of Wireshark that applies to industrial protocols using CIP Filters

6.11 Identify the source of cable and device faults in a DLR

6.11.a Tools – control Logix, ETAP, device web pages

6.12 Identify methods for troubleshooting a communication problem in a ProfiNET environment

6.12.a Look at SIMATIC STEP 7

6.12.b Is the cable is plugged into the right port

6.12.c Is the port configured for the proper VLAN speed duplex

6.12.d Are there port errors

6.12.e What is the status of the port

6.12.f Are there gateway IP problems

6.12.g Are there end point problems

6.12.h Is port connectivity verified

6.12.i Is it configured for the right VLAN

6.13 Troubleshoot ProfiNET using SIMATIC STEP 7 to view network topology, use the switch command line:

6.13.a Identify that ProfiNET is enabled on the switches and is configured correctly

6.13.b Ensure ProfiNET device switch interfaces are configured in the correct ProfiNET VLAN

6.13.c Check LLDP and ProfiNET LLDP switch databases to ensure that devices are recognized

6.13.d Use ProfiNET debug and status commands to ensure correct connectivity

6.13.e Use Wireshark to capture and identify non-real time and real-time traffic