PassQueen
a.k.a dumpsqueen.com

IoT Connected Factory for Systems Engineers Exam

Cisco 500-801

Version Demo

Total Demo Questions: 7

Total Premium Questions: 74

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Cisco IoT Connected Factory Overview	17
Topic 2, Cisco IoT Connected Factory Architecture	41
Topic 3, Cisco IoT Connected Factory Components	15
Topic 4, Mix Questions	1
Total	74

QUESTION NO: 1

Which three options are Cisco strengths in discrete manufacturing? (Choose three.)

A. use of open, unmodified standards

B. breadth and depth of industrial, ruggedized, converged network offerings

C. manufacture production line equipment

D. lowest cost option

E. professional services for full assessment, design, and implementation

F. cloud analytics

ANSWER: A B E

Explanation:

Cisco's strengths in discrete manufacturing center on an open industrial-network architecture, purpose-built infrastructure, and lifecycle expertise. The **use of open, unmodified standards** supports interoperability between information-technology and operational-technology environments, allowing manufacturers to integrate industrial assets and applications without relying on proprietary protocol changes. Cisco's industrial networking approach emphasizes standards-based Ethernet, IP, and security capabilities that can be deployed consistently from plant-floor devices through enterprise services.

The **breadth and depth of industrial, ruggedized, converged network offerings** is also a core strength. Cisco provides industrial Ethernet switching, wireless, routing, security, and network-management capabilities designed for challenging manufacturing conditions and for converging machine, control, and enterprise traffic on resilient infrastructure. This enables reliable connectivity and scalable segmentation across production environments.

Finally, **professional services for full assessment, design, and implementation** is important because manufacturing transformations require more than hardware. Cisco and its qualified partners can assess operational requirements, develop validated designs, deploy the solution, and support lifecycle operations. This combines industrial networking technology with practical expertise for secure, available connected-factory deployments. See Cisco's Manufacturing solutions and Industrial IoT solutions.

QUESTION NO: 2

Which option is essential in designing a Connected Factory solution for a discrete manufacturing customer?

A. understanding the customer's business outcomes and manufacturing objectives

B. uncompromising adherence to the Cisco Smart Business Architecture

C. designing the solution so that Cisco Professional and Technical Services are required

D. ensuring that Optimization Services are required after initial implementation

ANSWER: A

Explanation:

Understanding the customer's business outcomes and manufacturing objectives is essential because a Connected Factory design must start with the operational value the manufacturer needs to achieve. In discrete manufacturing, those outcomes can include improving overall equipment effectiveness, increasing production throughput, reducing unplanned downtime, improving product quality and traceability, strengthening worker safety, or enabling more flexible production. These priorities determine which operational technology data must be collected, how securely IT and OT systems must interconnect, and which applications, analytics, and network capabilities are needed.

Cisco's industrial networking approach emphasizes aligning technology architecture with operational requirements while accounting for plant availability, segmentation, security, and lifecycle needs. A design based on documented business and manufacturing objectives gives stakeholders measurable success criteria and helps ensure that the resulting network

supports production processes rather than merely deploying technology. It also enables an appropriate phased implementation plan, with the most valuable use cases addressed first. Cisco describes industrial networking and connected-manufacturing capabilities at Cisco Manufacturing Solutions and provides industrial network design resources through the Cisco Industrial IoT portfolio.

QUESTION NO: 3

Which Connected Factory Wireless solution architecture uses stand-alone access to implement WLAN functions of management, control, data transport, and client access?

A. Workgroup Access

B. Autonomous Access

C. Controlled Access

D. Unified Access

E. Normal Access

ANSWER: B

Explanation:

Autonomous Access is the Connected Factory Wireless architecture in which each access point operates as a stand-alone WLAN device. The access point locally performs the WLAN functions identified in the question: management of its own configuration, radio and client control, transport of wireless data, and client connectivity. This model is appropriate where a simple, self-contained wireless deployment is needed, such as a small or isolated industrial cell, and where centralized wireless-controller services are not required. Cisco describes autonomous access points as devices that contain the complete Cisco IOS software image and can be configured and managed individually; their operation does not depend on joining a wireless LAN controller. In a connected-factory context, this permits an access point to provide wireless service independently at the location where it is installed. The architecture is therefore defined by stand-alone access-point operation, rather than controller-based management or a distributed access design. Cisco's overview of autonomous access-point deployment and the associated configuration guidance are available in Cisco's autonomous versus lightweight AP documentation and the Cisco access point getting-started guide.

QUESTION NO: 4

Which two options are drawbacks to wireless media compared to wired methods? (Choose two.)

A. higher security

B. latency and jitter

C. packet loss

D. faster data transmission

E. lower costs

ANSWER: B C

Explanation:

latency and jitter and **packet loss** are drawbacks of wireless media when compared with a properly designed wired connection. Wireless frames travel through a shared radio-frequency medium and are subject to changing signal conditions, interference, attenuation, multipath effects, and contention for airtime. These conditions can cause transmission retries and variable delivery times. The resulting variation in packet arrival time is jitter, while the additional time consumed by contention, retries, and rate adaptation contributes to latency. Such variability is especially important for industrial IoT applications that require predictable communications, including control, automation, voice, and real-time telemetry.

Packet loss can occur when a wireless signal is too weak or corrupted for successful reception, when interference affects a transmission, or when retransmission attempts are exhausted. Although Wi-Fi mechanisms can retry frames to improve reliability, those retries themselves add delay and do not guarantee delivery under poor RF conditions. Cisco's industrial wireless guidance emphasizes RF planning, coverage, capacity, and interference management because these factors directly affect reliability and performance. Cisco also describes latency and packet loss as key network-quality characteristics for traffic that needs consistent service. See Cisco: What Is Wi-Fi? and Cisco: What Is a Wireless LAN?.

QUESTION NO: 5

Which option is the primary purpose of network segmentation in a cell/area zone?

A. Limit communications to required traffic flows between industrial assets.

B. Eliminate the need for firewall policy enforcement.

C. Allow all devices to share one broadcast domain.

D. Replace operational change-management processes.

ANSWER: A

Explanation:

Limit communications to required traffic flows between industrial assets. is correct because segmentation groups assets according to their operational role and security requirements, then applies policy at the boundaries between groups. This limits unnecessary connectivity, reduces the potential scope of a disruption, and supports defense in depth without preventing authorized control and supervisory communications. See Cisco Industrial Security.

QUESTION NO: 6

Which three actions help maintain availability when changes are required in an industrial network? (Choose three.)

A. documenting dependencies and communication flows before the change

B. testing the change in a representative environment when possible

C. preparing a rollback plan and maintenance window

D. making unannounced changes during active production

E. disabling monitoring until the change is complete

ANSWER: A B C

Explanation:

Documenting dependencies and communication flows before the change helps identify systems that could be affected by a configuration, software, or topology modification. **Testing the change in a representative environment when possible** reduces risk by validating the intended behavior before it reaches a production process. **Preparing a rollback plan and maintenance window** ensures that the organization can restore the previous state quickly if an unexpected issue occurs and that operational stakeholders are prepared for the work. Industrial changes must be coordinated with OT personnel because even a short communications interruption can affect production, quality, safety procedures, or equipment recovery. Cisco lifecycle guidance and industrial best practices emphasize disciplined planning, validation, and operational coordination for production network changes. See Cisco Services and NIST SP 800-82 Rev. 3.

QUESTION NO: 7

Which protocol is proprietary to Cisco and enables multiple paths in the network while preventing network loops?

A. Internal Message Access Protocol

B. Resiliency Ethernet Protocol

C. Ethernet Multi-Stream Protocol

D. Network Loop Prevention Protocol

ANSWER: B

Explanation:

Resiliency Ethernet Protocol refers to Cisco's Resilient Ethernet Protocol (REP), a Cisco-proprietary Layer 2 resiliency protocol. REP is designed for Ethernet access and aggregation topologies in which physical redundancy is needed without allowing a Layer 2 forwarding loop. Devices participating in a REP segment exchange control information, detect the segment topology, and place one interface into an alternate, nonforwarding state when necessary. This preserves a loop-free forwarding path while retaining redundant links that can be used if an active link or node fails. When a failure occurs, REP can unblock the appropriate alternate port and restore connectivity rapidly, making it well suited to resilient industrial and metro-Ethernet-style ring deployments. Cisco documents REP as providing an alternative to spanning-tree-based loop prevention for supported ring and segment designs, while maintaining redundant paths for availability. The protocol's Cisco-specific implementation is the key identifying characteristic in the question. See Cisco's Resilient Ethernet Protocol configuration guidance and its REP technical overview.