DUMPSARENA

HCIP-Access V2.5

Huawei H35-211_V2.5

Version Demo

Total Demo Questions: 8

Total Premium Questions: 88

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

(Multiple choice) When the OLT main control board CPU is detected to be continuously elevated, the following possible causes are?

A. The user logged in illegally

B. Network loops

C. Cyber attacks

D. Rogue ONU

ANSWER: A B C D

Explanation:

All listed conditions can plausibly sustain high CPU utilization on an OLT main control board. An illegal user login, particularly when associated with repeated authentication attempts, unauthorized management access, or command activity, consumes control-plane resources used for login processing, session management, auditing, and CLI or management-protocol handling. Network loops can generate large volumes of repeated Layer 2 traffic and protocol processing, placing continuous load on the OLT control plane. Cyber attacks, especially scanning, flooding, malformed-packet, and denial-of-service traffic directed at management or control interfaces, can similarly exhaust CPU resources. A rogue ONU may repeatedly attempt registration, send abnormal PON control traffic, or otherwise create excessive ONU-management events; these events must be processed by the OLT and can keep main-control CPU usage elevated. In operational troubleshooting, Huawei recommends checking CPU usage together with alarms, ONU status, traffic statistics, management-login records, and security logs so that the sustained control-plane load can be correlated with its source. Huawei's optical-access product documentation and support resources are available through the Huawei MA5800 support page and the Huawei Enterprise Support Center.

QUESTION NO: 2

(Radio) A power access service deploys GPON Type C dual attribution protection, and the protection group is fixed with the upstream Ethernet port status on the OLT, and when the Ethernet port status associated with the protection group on the OLT becomes down, the following description is incorrect.

A. The state of the ONU-side working port changes to standby.

B. The OLT detects the ONU uplink-state change.

C. After switchover, ONU service is sent to the OLT through the protection port; that is, service packets are transmitted over the protection path.

D. The ONU detects link failures and triggers protection reversals.

ANSWER: D

Explanation:

The ONU detects link failures and triggers protection reversals is the incorrect description. In this scenario, the protection group is explicitly associated with the status of an upstream Ethernet port on the OLT. Therefore, an Ethernet-port-down event is detected locally by the OLT, which is the device that evaluates the configured trigger condition and performs the corresponding protection-control action. The event is not an ONU-detected PON-side link failure. After the OLT initiates the relevant protection state transition, the ONU receives the control behavior required for the Type C dual-homing protection arrangement and forwards service through the selected available path. This distinction matters operationally: the configured trigger source is the OLT uplink Ethernet interface, rather than loss of optical signal, ONU Ethernet-link detection, or an autonomous ONU switching decision. GPON Type C protection is intended to maintain service availability through redundant OLT/PON resources, with protection behavior coordinated by the access-network equipment and its configured protection policy. GPON system architecture and protection-related requirements are defined in the ITU-T GPON recommendations, including ITU-T G.984.1. Huawei's optical access platform information is available at Huawei Optical Access Network.

QUESTION NO: 3

(Radio) When deploying GPON Type C single attribution protection, the following description is correct.

A. The branch fiber breaks, and the state of the OLT's work port becomes standbY

B. Two ports protected by the OLT side cannot send and receive data at the same time

C. When the olt uplink fails, a protection reversal can be triggered

D. The service configuration of ONU access is completely identical to the configuration before protection

ANSWER: B

Explanation:

“Two ports protected by the OLT side cannot send and receive data at the same time” is correct because GPON Type C single-homing protection provides a protected active/standby PON forwarding relationship at the OLT side. The two associated GPON ports provide redundant access paths, but a given ONU service is carried through the currently active protection path. The standby path is maintained as a backup and takes over service forwarding when a protection-switching condition is detected. This design prevents duplicate downstream transmission toward the ONU and prevents simultaneous upstream reception/processing for the same protected service on both members of the protection pair. It also ensures that the ONU has one effective serving PON path at a time, preserving normal GPON registration, bandwidth allocation, and service forwarding behavior during steady-state operation and after a protection switchover. The ITU-T GPON architecture defines the protection concepts used by GPON systems, while Huawei’s optical access portfolio implements these mechanisms through OLT and PON protection features. See ITU-T G.984.1: Gigabit-capable passive optical networks and Huawei PON optical networking.

QUESTION NO: 4

When ont fails or the hardware needs to be replaced, the ONT service needs to be replaced, and then the ONT service needs to be removed on the OLT, and then the new ONT service needs to be registered

A. wrong

B. Right

ANSWER: A

Explanation:

wrong is correct because deleting the existing ONT and registering a new ONT as a routine replacement procedure is not the recommended service-preservation method. Huawei OLTs provide an ONT replacement mechanism, commonly performed with the `ont replace` operation, that associates the replacement device with the existing ONT record. This is designed to retain the original ONT’s relevant configuration and service provisioning, minimizing the need to recreate service-port, VLAN, GEM-port, and related access-service settings after hardware replacement. The replacement workflow is particularly valuable in production networks because it reduces restoration time and avoids unnecessary service reprovisioning errors. The technician should confirm that the replacement ONT is compatible with the original deployment and use the OLT’s supported replacement procedure according to the platform software version and authentication method. Huawei’s optical-access product documentation and command references are available through the Huawei MA5800 product support page and the Huawei Enterprise documentation portal. Therefore, the stated mandatory sequence of removing the old ONT service and newly registering all service configuration does not describe the standard ONT replacement approach.

QUESTION NO: 5

(Multi-select) Which of the following PPP authentication protocols can be used during a PPPoE session?

A. PAP

B. CHAP

C. PADI

D. IGMP

ANSWER: A B

Explanation:

PAP and **CHAP** are correct. PPPoE encapsulates PPP frames over Ethernet, and PPP authentication can be performed after the PPPoE discovery and session-establishment phases. PAP performs authentication by sending a user name and password to the peer, whereas CHAP uses a challenge-response mechanism and does not send the password itself in clear text. PADI and PADR are PPPoE discovery messages rather than PPP authentication protocols, and IGMP is used for multicast group membership management. See RFC 2516 for PPPoE, RFC 1334 for PAP, and RFC 1994 for CHAP.

QUESTION NO: 6

(Multi-select) esight is a network management software positioned in the enterprise network scenario, which can view the details of onu devices, including the following information?

A. UNT port information

B. speed

C. Optical module temperature

D. The optical module transmits power

ANSWER: A B C D

Explanation:

eSight provides device-level visibility for managed ONU equipment, combining inventory, interface status, and optical-transceiver monitoring data in the ONU detail view. **UNT port information** is included because the management platform must show the ONU's user-network interfaces, their operational state, and associated service-facing characteristics. **speed** is also available as a port attribute, allowing an administrator to identify the interface rate or negotiated link rate when checking ONU connectivity and service status.

For optical access troubleshooting, eSight can obtain digital diagnostic monitoring information reported by the ONU optical transceiver. Consequently, **Optical module temperature** is displayed as an environmental health indicator for the module, while **The optical module transmits power** provides the upstream optical-power reading needed to assess the optical link and identify attenuation or transceiver issues. These values support centralized monitoring of ONU access ports and their optical uplinks. Huawei's eSight documentation and product support resources describe the platform's device management, port monitoring, and optical monitoring capabilities: Huawei eSight product support and Huawei eSight documentation.

QUESTION NO: 7

(Single choice) In a GPON system, which T-CONT type provides assured bandwidth and non-assured bandwidth?

A. Type 1

B. Type 2

C. Type 3

D. Type 4

ANSWER: C

Explanation:

Type 3 is correct. GPON T-CONTs are used to carry upstream traffic and define the bandwidth-allocation behavior for an ONU. A Type 3 T-CONT supports assured bandwidth, which is allocated after fixed bandwidth requirements are met, and non-assured bandwidth, which can be assigned when unused upstream capacity is available. This model is suitable for services requiring a committed bandwidth component while still allowing additional bandwidth when the PON has spare capacity. Type 1 provides fixed bandwidth only, Type 2 provides assured bandwidth, and Type 4 provides best-effort bandwidth. The T-CONT bandwidth types are defined in ITU-T Recommendation G.984.3.

QUESTION NO: 8

The scope of protection of the (multiple choice) GPON Type B dual attribution protection includes

A. Primary and standby OLTs

B. Primary and standby primary thousand fibers

C. OIT's primary and standby PON should be ports

D. Primary and standby branch fibers

ANSWER: A B C

Explanation:

GPON Type B dual-homing protection establishes two upstream parent paths for the protected PON service. Therefore, **Primary and standby OLTs** are included when the dual-homing design uses separate parent OLTs, ensuring that an active service path can be provided through the standby parent side. **Primary and standby primary thousand fibers** refers to the primary and standby feeder-fiber paths between the OLT side and the splitter side. These separate feeder paths are a fundamental part of Type B protection, because a feeder-side interruption can be bypassed by switching to the alternate upstream optical route.

OIT's primary and standby PON should be ports identifies the paired OLT PON interfaces that terminate the two protected upstream paths. The Type B architecture uses these active/standby PON-side resources together with the paired feeder fibers to maintain service continuity at the PON access layer. This protection model is based on the GPON protection architecture defined for duplicated OLT/PON-side and feeder-side connectivity; the applicable GPON system framework is specified by the ITU-T in Recommendation G.984.1. Huawei’s optical-access portfolio and OLT architecture information is available at Huawei Optical Line Terminals.