Huawei.H35-211_V2.5.v2026-06-18.q56

Exam Code:	H35-211_V2.5
Exam Name:	HCIP-Access V2.5
Certification Provider:	Huawei
Free Question Number:	56
Version:	v2026-06-18
# of views:	107
# of Questions views:	560
https://www.freecram.net/torrent/Huawei.H35-211_V2.5.v2026-06-18.q56.html	

NEW QUESTION: 1
The Class D multicast address range is from 224.0.0.0 to 238.255.255.255.
A. True
B. False
Answer: (SHOW ANSWER)
IPv4 multicast (historically "Class D") occupies the address block 224.0.0.0 through 239.255.255.255. Any upper bound of 238.255.255.255 is incorrect because it excludes the full 239/8 administratively scoped range.
This is standardized in the IANA IPv4 Multicast Address Space registry and reflected in foundational multicast specifications.

NEW QUESTION: 2
(Radio) When using the SIP protocol, a local digitmap is used for matching. If you use the default matching mode to match a 7-digit number beginning with 7727, which of the following configurations is valid?
A. local-digitmap add huawei normal 7727xxx/7726.
B. local-digitmap add huawei normal 772./7727xxx
C. local-digitmap add huawei normal 7727
D. local-digitmap add huawei normal 7727xxx/7727
Answer: (SHOW ANSWER)
Huawei digitmap syntax uses x to represent any single digit 0-9. To match a 7-digit number starting with
7727, the correct pattern is 7727xxx.
A adds an unrelated rule 7726. and uses . incorrectly as a wildcard; not recommended.
B uses 772. (invalid for the intended match) plus 7727xxx; the first part is improper.
C matches only the 4-digit string 7727.

D contains 7727xxx (correct) and an additional 7727 rule; although the extra rule is unnecessary, it does not prevent correct matching.
References: HCIP-Access V2.5 Study Guide - Voice access configuration, local digitmap syntax (x as digit,
/ as rule separator) and default matching behavior.

NEW QUESTION: 3
The OLT is configured to use IGMP Version 2. When the OLT receives an IGMPv3 Join (Report) message forwarded from an ONT, what action will it take?
A. Normal forwarding
B. Send a specific-group query message
C. Send a general (universal) group query message
D. Discard directly
Answer: (SHOW ANSWER)
Huawei multicast guidance stresses IGMP version compatibility: devices running an earlier version must interoperate only with hosts using the same or earlier version, otherwise v3 messages may not be processed.
In Huawei's multicast feature guidance for access devices (OLT side vs. user side), the behavior documented is that when the device is operating in IGMPv2, IGMPv3 Report messages from terminals are not processed- interoperation is restored only after the terminal/device side is downgraded to v2 (often driven by periodic queries that induce hosts to respond in v2). This maps operationally to dropping unsolicited IGMPv3 Reports when the OLT is fixed to v2. Huawei also recommends ensuring the device runs an IGMP version the same as or later than member hosts to avoid such loss. Therefore, with OLT fixed at v2, an incoming v3 Join is discarded.

NEW QUESTION: 4
OLT can perform traffic shaping through service-port.
A. True
B. False
Answer: (SHOW ANSWER)
On Huawei OLTs, the service-port is a binding between the user-side access (ONT/port) and a VLAN/GEM channel, and it supports traffic policing (CAR/rate-limit) by referencing a traffic/queue profile. Traffic shaping (buffer-based smoothing, token bucket with queue drain) is provided on ports/queues or GEM/LLID directions, not on the service-port object itself. Therefore, shaping is not performed via the service-port; applying a traffic profile there enforces policing, not shaping.
References: HCIP-Access V2.5 Study Guide - OLT QoS Concepts (service-port policing vs port/queue shaping); Huawei OLT QoS & Traffic Management Configuration - service-port CAR and port/GEM shaping behavior.

NEW QUESTION: 5

If a customer needs to protect the ONU trunk optical path but does not need to protect the ONU branch optical paths, which PON line protection mode should be used?

A. Type D

B. Type B

C. Type C

D. Type A

Answer: (SHOW ANSWER)

In Huawei GPON/EPON protection planning, Type B protection uses two PON ports on the same OLT with dual feeder (trunk) fibers into the same ODN. It protects the OLT PON port and the feeder/trunk optical path while branch/distribution fibers to ONUs are not protected. This exactly matches the requirement "protect trunk; do not protect branches." References: HCIP-Access V2.5 Study Guide - PON Line Protection (Type A/B/C definitions and protection scope).

NEW QUESTION: 6

When configuring IPTV services on the U2000, what templates are included in the IGMP templates?

A. Permission templates

B. Multicast user templates

C. Program templates

D. Preview parameter template

Answer: (SHOW ANSWER)

In U2000's IPTV/IGMP service model, the IGMP template suite includes: Permission templates (program authorization), Multicast user templates (user IGMP attributes), Program templates (program/group definitions), and Preview parameter templates (preview/fast-zapping parameters). These cooperate to control user authorization, program mapping, and IGMP behavior. References: HCIP-Access V2.5 Study Guide - IPTV over PON with U2000; U2000 Multicast/IGMP Configuration Templates (permission, user, program, preview).

NEW QUESTION: 7

(Radio) The following is not a QoS service model is

A. DiffServ

B. IntServ

C. FIFO service

D. Best Effort

Answer: C (LEAVE A REPLY)

In Huawei's QoS theory (aligned with IETF), the recognized service models are Best Effort, Integrated Services (IntServ), and Differentiated Services (DiffServ). FIFO is a queueing discipline (scheduling method) rather than a service model. FIFO simply forwards packets in arrival order without classification or guarantees, and while it can be used within Best Effort, it is not itself a service model.

References: HCIP-Access V2.5 Study Guide - QoS Fundamentals; Huawei VRP QoS Configuration Guide - Service Models vs. Queue Scheduling.

NEW QUESTION: 8
If a rogue ONU exists on a PON port of the OLT and has gone online, another ONT or all ONTs connected to the same PON port may go offline or go online and offline frequently.
A. TRUE
B. FALSE
Answer: (SHOW ANSWER)
A rogue ONU that transmits out of schedule or at abnormal optical levels can disrupt upstream time-slotting on the PON, causing collision and interference. This can force other ONUs on the same PON to deregister or flap frequently. Huawei OLTs provide rogue ONU detection/isolation to protect the PON.
References: HCIP-Access V2.5 Study Guide (PON Faults-Rogue ONU Impact and Handling); Huawei OLT Maintenance Guide (Rogue ONU detection and isolation).

NEW QUESTION: 9
Which of the following statements about the E2E ODN pre-connection solution are correct?
A. Easy deployment, 100% splicing-free, no need for professional skills and tools, and improved efficiency
B. Splitters are installed in pre-connected boxes and occupy small space.
C. The pre-connection solution uses distributed optical splitting to reduce the number of drop cables, thereby reducing the number of pipes and cables.
D. Easy to maintain, no need for fiber splicing, and low maintenance skill requirements
Answer: (SHOW ANSWER)
Huawei's E2E pre-connection ODN (pre-connectorized ODN) adopts factory-pre-terminated cables, closures and splitter modules. Features highlighted in HCIP-Access V2.5 include: splicing-free quick installation (raising build efficiency and reducing skill/tool dependence), compact pre-connected splitter boxes, distributed splitting that shortens drop lengths and reduces ducts/cables, and easy O&M because modules are plug-and-play with no field splicing.
References: HCIP-Access V2.5 Study Guide - ODN Construction Solutions (Pre-connection/E2E), ODN Engineering and Maintenance Guidelines - features & advantages of pre-connectorized ODN.

NEW QUESTION: 10
Which one of the following protection schemes can provide OLT-level protection?
A. Type B dual-homing
B. Ethernet port protection group
C. LACP
D. Type B single-homing
Answer: (SHOW ANSWER)

OLT-level (device-level) protection is achieved by dual-homing ONUs to two independent OLT interfaces so that services can switch to another OLT when one fails. In Huawei protection taxonomy, the dual-homing scheme (as contrasted with single-homing) provides device-side redundancy for the OLT. By comparison, Ethernet port protection groups and LACP protect uplink links and bandwidth at Layer 2, not the OLT device itself; single-homing does not protect against OLT failure.
References: HCIP-Access V2.5 - Protection Schemes and Capabilities; OLT Protection Deployment Guide - Dual-homing vs. Ethernet/LACP Link Protection.

NEW QUESTION: 11
Assume that there are 500 broadband users with a concurrency rate of 40%, penetration rate of 50%, online bandwidth of 4 Mbit/s, duty cycle of 12.5%, 1 channel, and coverage rate of 70%. Then the bandwidth is 35 Mbit/s.
A. TRUE
B. FALSE
Answer: (SHOW ANSWER)
In capacity planning, the planned bandwidth is computed as:
Planned Bandwidth = Users × Penetration × Concurrency × Online Bandwidth × Duty Cycle × Channels × Coverage.
Substituting the values: 500 × 0.5 × 0.4 × 4 Mbit/s × 0.125 × 1 × 0.7
= 250 × 0.4 × 4 × 0.125 × 0.7
= 100 × 4 × 0.125 × 0.7
= 400 × 0.125 × 0.7
= 50 × 0.7
= 35 Mbit/s.
This matches the given result, so the statement is true.

NEW QUESTION: 12
(Single) A total of 100 multicast users on an OLT are watching 20 multicast programs. Assuming that each multicast program occupies 2 Mbit/s bandwidth, how much multicast traffic is currently on the OLT upstream port?
A. 200 Mbit/s
B. 100 Mbit/s
C. 40 Mbit/s
D. 50 Mbit/s
Answer: (SHOW ANSWER)
In IP multicast, only one copy per multicast group (program) is forwarded upstream, regardless of how many users are watching it. Replication happens downstream at the access/edge, not toward the core. Therefore the upstream traffic equals the number of active multicast groups × per-group bitrate:
20 programs × 2 Mbit/s = 40 Mbit/s.

This behavior is consistent with Huawei's multicast feature descriptions and general multicast principles (IGMP/PIM), which explain that multicast traffic is sent as a single flow per group and replicated only where branching occurs, not multiplied by user count.

NEW QUESTION: 13
In the GPON system, Huawei recommends that optical splitting levels do not exceed 2. Which of the following networking is incorrect?
A. Level-1 optical splitting 1:2, Level-2 optical splitting 1:16
B. Level-1 optical splitting 1:16, Level-2 optical splitting 1:16
C. Level-1 optical splitting 1:8, Level-2 optical splitting 1:8
D. Level-1 optical splitting 1:2, Level-2 optical splitting 1:8
Answer: (SHOW ANSWER)
Huawei GPON design recommends at most two splitting stages and a total split ratio within the optical power budget (commonly up to 1:64 for standard budgets).
A: 1:2 × 1:16 = 1:32 (valid).
C: 1:8 × 1:8 = 1:64 (valid under standard budgets).
D: 1:2 × 1:8 = 1:16 (valid).
B: 1:16 × 1:16 = 1:256, which exceeds typical GPON budgets and recommended engineering practice. Hence B is the incorrect networking.

NEW QUESTION: 14
Which of the following multicast protocols is directly associated with the hosts? Specifically, routers running the protocol manage the joining and leaving of hosts in a multicast group and send multicast data to the hosts by querying the multicast forwarding table.
A. PIM-DM
B. MSDP
C. PIM-SM
D. IGMP
Answer: D (LEAVE A REPLY)
IGMP is the host-side membership protocol: the first-hop router (querier) uses IGMP Queries/Reports/Leaves to manage host participation in multicast groups and to ensure forwarding state reflects receiver interest. PIM- DM/PIM-SM build distribution trees between routers, and MSDP shares source information between PIM- SM domains-they are not used by hosts.
References: HCIP-Access V2.5 - Multicast Protocol Roles (IGMP vs. PIM/MSDP); Huawei Multicast Configuration Guide - Host Membership with IGMP.

NEW QUESTION: 15
If the ONT zero-touch provisioning function is enabled on eSight, you can configure multiple service profiles.
Which parameters can be set on the Multi-Service Profile Management tab page?

A. Default VLAN
B. ONU type
C. Number of Ethernet ports
D. VLAN
E. Voice VLAN
Answer: (SHOW ANSWER)
In eSight's ONT Zero-Touch workflow, multi-service profiles define service parameters delivered to ONTs- primarily service VLANs such as Internet/Data VLAN, Voice VLAN, and IPTV/Multicast VLAN with related QoS. Hardware attributes like ONU type or Ethernet port count are part of the device/ONT profile, not the multi-service profile. A generic "Default VLAN" parameter is not used here; instead, explicit service VLANs are specified (for example, data VLAN and voice VLAN).
References: HCIP-Access V2.5 Study Guide - Network Management & Maintenance: eSight ONT Zero- Touch (multi-service profile content: data/voice/multicast VLAN parameters, QoS templates).

NEW QUESTION: 16
Which of the following statements about multicast is incorrect?
A. General parameters for multicast protocols (IGMP proxy and IGMP snooping) are configured globally at Layer 2 and apply to all multicast VLANs.
B. The report sent by a user is captured by the board logic and sent to the CPU of the board.
C. You can add IGMP users to a BTV. By default, a multicast user can watch 8 programs.
D. In the case of IGMP match mode disable, you need to configure a multicast channel.
Answer: D (LEAVE A REPLY)
A is consistent with Huawei L2 multicast practice: global L2 multicast/IGMP snooping parameters can be set and then take effect for multicast VLANs involved in service provisioning.
B reflects the forwarding/CPU-punt behavior on access line cards: IGMP Reports/Leaves from users are recognized by board logic and processed by the control plane to update multicast state.
C matches default service control on BTV/IPTV access where a default program limit (commonly 8) per user applies unless adjusted by policy/profile.
D is incorrect: when IGMP match mode is disabled, multicast programs are not required to be pre-provisioned as channels; groups can be learned dynamically by IGMP. Preconfiguring channels is needed when match mode is enabled (channel matching enforced).
References: HCIP-Access V2.5 - Multicast Service Provisioning on OLT/MDU; Huawei BTV/Multicast Feature Guide - IGMP Snooping/Proxy, Program Limits, and Match-Mode Behavior.

NEW QUESTION: 17
In the NGN system, the ( ) adopts the packet technology to provide a unified integrated transmission platform with high reliability, QoS guarantee, and large capacity.
A. Network control layer
B. Core switching layer
C. Service management layer
D. Edge access layer
Answer: (SHOW ANSWER)
In NGN architectures, services (voice, video, data) converge over a packet-based backbone. The core switching layer provides the unified transport using IP/MPLS and related QoS mechanisms, delivering high reliability and large-capacity switching for all upper-layer services. The control and management layers orchestrate services, while the edge/access layer aggregates users-but the packet-based integrated transmission platform itself is the role of the core.
References: HCIP-Access V2.5 study content (NGN overview, layered architecture, and packet-based core transport responsibilities).

NEW QUESTION: 18
(Radio) Follow the multicast IP address 227.120.1.32. The correct multicast MAC address corresponding to it is:
A. 01-00-5e-78-01-32
B. 01-00-5e-14-01-20
C. 01-00-5e-78-01-20
D. 01-00-5e-14-01-32
Answer: C (LEAVE A REPLY)
For IPv4 multicast, the destination MAC is derived by mapping the lower 23 bits of the multicast IP address into the OUI 01-00-5E. The 4th MAC byte is the lower 7 bits of the IP's second octet (so it ranges 00-7F), and the 5th and 6th MAC bytes are the third and fourth IP octets directly:
Multicast OUI: 01-00-5E
IP: 227.120.1.32
2nd octet = 120 (0x78). Its lower 7 bits are still 0x78 (since the MSB is 0).
3rd octet = 1 (0x01)
4th octet = 32 (0x20)
Therefore the MAC is 01-00-5E-78-01-20 # option C.
(This mapping aligns with standard IPv4 multicast-to-Ethernet rules described in Huawei's multicast overview sections in HCIP-Access materials and Huawei OLT product guides.)

NEW QUESTION: 19

(Single choice) The following statement about the PITP protocol is incorrect
A. The PITP protocol includes PITP P mode and PITP V mode
B. The purpose of the PITP feature is to provide the upper authentication server with the physical location information of the access user, and the BRAS device can realize the user account and the press position after obtaining the user access location information
C. Bind the authentication of the information to avoid the theft and roaming of the user account
D. In PITP V mode, the user's physical location information is added to the PPPoE message sent by the user side to cooperate with the upper-level server for user authentication
E. PITP P mode can also be called PPPoE+ mode
Answer: (SHOW ANSWER)
PITP (Port Identification Transparent Transmission) is used on access networks to carry a user's physical access-location to the upper AAA/BRAS. It has two working forms: P-mode (PPPoE+)-injecting location identifiers into PPPoE discovery-and V-mode (Vendor-tag)-carrying vendor/location tags transparently upstream. The purpose is to let the upper server associate user credentials with access location and, by policy, restrict roaming. Options A, B, D, and E correctly describe these behaviors/terms. Option C is inaccurate as written: PITP itself does not "bind the authentication" or inherently "avoid theft/roaming"; it only delivers location info. Preventing credential theft/roaming is achieved by AAA/BRAS policy that uses the PITP- carried location, not by PITP alone.

NEW QUESTION: 20
The DBA scheduling of the GPON system is only for the upstream traffic, and the downstream traffic cannot be scheduled.

A. True
B. False
Answer: (SHOW ANSWER)
In GPON, DBA (Dynamic Bandwidth Allocation) operates in the upstream direction. The OLT grants upstream transmission opportunities to ONTs by assigning T-CONT bandwidth (Fixed/Assured/Non-Assured
/Best-Effort) within upstream frames. The downstream direction is a continuous broadcast stream from the OLT at the fixed GPON line rate; user traffic is multiplexed without DBA. Hence, DBA is upstream-only; downstream traffic is not DBA-scheduled.
References: HCIP-Access V2.5 Study Guide - GPON DBA Mechanism (T-CONT types and upstream grants); GPON Traffic Management Overview - upstream DBA vs downstream broadcast.

NEW QUESTION: 21
(Radio) In the ACL, if you need to filter packets by source IP, destination IP, and port number, the ACL number template to create is:
A. 5000-5999
B. 3000-3999

C. 2000-2999
D. 4000-4999
Answer: (SHOW ANSWER)
On Huawei VRP, Advanced IPv4 ACLs (which can match source IP, destination IP, and L4 port numbers) use the 3000-3999 numbering range.
2000-2999 = Basic IPv4 ACL (matches source IP only).
3000-3999 = Advanced IPv4 ACL (matches source/destination IP, protocol, ports).
4000-4999 = Layer 2 (MAC) ACL.
5000-5999 = User-defined/other ranges, not the standard advanced IPv4 range.
Therefore, to match IPs and ports, select 3000-3999.
References: HCIP-Access V2.5 - ACL Principles and Numbering; Huawei VRP ACL Configuration Guide - IPv4 Basic vs. Advanced ACL Ranges.

NEW QUESTION: 22
(Single) When deploying home and guest services in a PON system, which of the following services has the highest priority?
A. VOIP
B. GAME
C. INTERNET
D. IPTV
Answer: A (LEAVE A REPLY)
In access networks, Huawei recommends prioritizing real-time voice (VoIP) traffic with the highest forwarding priority (typically EF, 802.1p 5) to ensure low latency and jitter. IPTV/video is generally next (AF classes), while gaming and general Internet browsing are treated lower than voice. Therefore, VOIP receives the top priority to protect call quality under congestion.
References: HCIP-Access V2.5 - QoS Service Planning on PON; Huawei OLT QoS Feature Guide - Traffic Classes and 802.1p/DSCP Mapping.

NEW QUESTION: 23
(Multi-select) VLAN planning principles need to be considered:
A. The total number of VLANs
B. Customer type and number of users
C. Type and quantity of services
D. Uplink networking mode
E. The networking topology of the OLT
Answer: (SHOW ANSWER)
Huawei VLAN planning considers overall VLAN scale, user categories and volume, service types (HSI/IPTV
/VoIP) and their isolation, uplink/aggregation mode (e.g., QinQ, VXLAN interwork), and device/topology constraints (e.g., OLT slot/board distribution). All listed factors affect VLAN count, tagging scheme, and scalability.

References: HCIP-Access V2.5 Study Guide (Campus and access VLAN design principles; service isolation and scalability).

NEW QUESTION: 24
(Radio) When the OLT global or VLAN service template enables the PITP switch, the service port allows the upstream packet to carry the Vendor tag, and the user side indeed carries vendor tag information. Which statement about OLT processing of PITP messages is correct?
A. OLT adds a local Vendor tag to the upstream PITP packet
B. OLT forwards the user-side PITP message directly without any processing
C. OLT retains the Vendor tag carried in the upstream PITP message and adds the local Vendor tag
D. OLT drops upstream PITP packets
Answer: (SHOW ANSWER)
With PITP enabled and Vendor-tag switching allowed, Huawei OLTs support transparent transmission and augmentation: the OLT keeps the user-carried Vendor tag and appends the local Vendor tag (e.g., slot/port
/location), ensuring the upstream AAA/BRAS receives both the access-side identity and the OLT's own location identity. Simply adding only the local tag (A) loses user-side info; forwarding unchanged (B) omits OLT location; discarding (D) contradicts the feature intent.

NEW QUESTION: 25
Which of the following options can improve the service experience of multicast users when switching channels (shorter switching time)?
A. When adding a multicast program, disable the pre-join feature
B. Enable Quick (Fast) Leave when adding a multicast user
C. When you add a multicast user, enable the preview feature
D. Use group addresses with small values
Answer: (SHOW ANSWER)
In IPTV/multicast access scenarios, channel zapping delay is heavily influenced by how fast the network stops forwarding the previous channel's stream after a user switches. Huawei documents the IGMP Fast Leave
/Prompt Leave feature, which enables the access device to immediately prune the old multicast group on receipt of a Leave (without waiting for group-specific queries and timers), thereby reducing the channel change delay and improving perceived switching speed. Option A explicitly disables a helpful pre-join optimization, which would worsen experience; Option C (preview) concerns showing brief previews and is not a primary mechanism for shortening zapping time; Option D is unrelated to performance. Thus, enabling Quick/Fast Leave is the correct action to shorten switching time.

NEW QUESTION: 26
Which of the following is a RADIUS feature?

A. The same transmission protocol as HWTACACS is used.
B. You can adjust the fields to be encrypted in packets according to user requirements.
C. After a user passes authentication, the returned message is different from that returned by the HWTACACS server.
D. RADIUS has reliable transmission.
Answer: (SHOW ANSWER)
A: Incorrect - RADIUS typically uses UDP (1812/1813), while HWTACACS/TACACS+ uses TCP (port
49).
B: Incorrect - In RADIUS, only the user-password attribute is encrypted; fields are not selectively encrypted by user choice. TACACS+ can encrypt the entire payload.
D: Incorrect - Because RADIUS uses UDP, transport is not inherently reliable.
C: Correct - RADIUS and HWTACACS differ in message structure and returned attributes after authentication (e.g., RADIUS attribute-value pairs for access control/QoS/VLAN vs. HWTACACS command
/privilege oriented responses). Thus the returned content/format differs between the two.
References: HCIP-Access V2.5 Study Guide - AAA overview and comparison of RADIUS vs HWTACACS (transport, encryption scope, response attributes).

NEW QUESTION: 27
Which of the following statements about the implementation of VLAN Layer 2 intercommunication through ARP proxy and VLAN service-profile is correct?
A. Compared with the VLAN service profile, ARP proxy saves IP addresses.
B. Both of them can implement Layer 2 isolation of smart VLANs.
C. The ARP proxy must be configured on the OLT to solve the voice interworking problem.
D. The VLAN service profile must be configured on the ONU to implement voice communication.
Answer: (SHOW ANSWER)
For intercommunication across VLANs-especially for voice between ONUs-ARP Proxy is configured on the OLT so the OLT responds to ARP on behalf of endpoints and bridges traffic across VLAN boundaries without exposing the full L3 gateway to each segment.
A: "Saving IP addresses" is not the defining difference; ARP Proxy's function is ARP mediation to enable L2
/L3 reachability.
B: Both features target intercommunication, not isolation.
D: A VLAN service-profile is planned and applied from the OLT side to ONUs; it is not "configured on the ONU" directly for this purpose.
References: HCIP-Access V2.5 (OLT-based ARP Proxy for voice interworking; VLAN service-profile application model).

NEW QUESTION: 28

In the evolution of EPON to 10G EPON, a smooth transition is achieved at the local end by adding WDM modules, and the ODN can be reused/coexist.

A. True

B. False

Answer: (SHOW ANSWER)

10G-EPON is designed for coexistence with EPON on the same ODN by using separate downstream wavelengths and dual-rate upstream mechanisms. Operators can realize a smooth upgrade at the OLT (local end) by inserting WDM mux/demux modules (or using dual-rate PON ports) while continuing to use the existing ODN fiber plant and splitters. This is a standard migration path emphasized in HCIP-Access materials for PON evolution.

References: HCIP-Access V2.5 Study Guide - Optical Access Overview, EPON # 10G-EPON evolution and coexistence; OLT Product & Technology Description - wavelength plan and WDM-based smooth upgrade.

NEW QUESTION: 29

(Single-choice) An IPTV user reports the TV cannot be watched. After enabling OLT debug for multicast

/IGMP, the printed information (authorization result) indicates the conclusion below. This can be judged by the results of the query:

A. The PON port multicast bandwidth is insufficient

B. The user does not have permission to watch the show

C. IGMP Snooping failure

D. User bandwidth validation failed

Answer: (SHOW ANSWER)

In Huawei IPTV access, when the OLT's IGMP audit/authorization debug shows a negative program-rights

/authorization result, it indicates that the user lacks permission for the requested multicast program group.

This is distinct from port multicast bandwidth alarms (insufficient multicast bandwidth), IGMP snooping state malfunctions, or subscriber traffic shaping/bandwidth checks. Authorization failures map directly to "no permission to watch the program." References: HCIP-Access V2.5 Study Guide - IPTV over PON, IGMP/Multicast Control and CAS/Program Authorization; Huawei OLT Multicast Service Configuration and Maintenance Guide - IGMP Join Authorization Diagnosis.

NEW QUESTION: 30

After anti-DoS attack is configured, the system periodically checks all user ports on the board. If the system detects attacks for multiple consecutive times, the system adds the corresponding port to the blacklist and waits for a random period before a new round of detection to determine whether to remove the port from the blacklist.

A. TRUE

B. FALSE

Answer: A (LEAVE A REPLY)

Huawei anti-DoS on access boards performs periodic detection. Ports with consecutive detections of abnormal traffic are placed into a blacklist/quarantine state. The system then applies a random back-off interval before re-detecting; if no further anomalies are found, the port can be automatically removed from the blacklist.

References: HCIP-Access V2.5 Study Guide - Security hardening on access devices (DoS protection, blacklist strategy, periodic detection).

NEW QUESTION: 31

On U2000, if an OLT PON port LED is not green, it indicates the PON port is faulty.

A. Wrong

B. Right

Answer: (SHOW ANSWER)

This is wrong. A PON port LED not green may indicate several states-not only a hardware fault. It can mean the port is administratively shutdown, no ONUs are registered, or the port is in an alarm or idle state depending on the LED color and blinking pattern. Fault requires correlation with alarms and performance counters in U2000, not LED color alone.

References: HCIP-Access V2.5-OLT maintenance and alarm interpretation; Huawei OLT Hardware Description & Indicator Guide (PON port LED states and meanings).

NEW QUESTION: 32

(Radio) A power access service deploys GPON Type C dual-attribution protection, and the protection group is bound to the uplink Ethernet-port status on the OLT. When the Ethernet port associated with the protection group on the OLT goes Down, the following description is incorrect.

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

B. The OLT detects the ONU uplink state change

C. After switchover, the ONU's service is sent to the OLT through the protect port (service traffic follows the protect path)

D. The ONU detects the link failure and triggers the protection switchover

Answer: (SHOW ANSWER)

In GPON Type C dual-attribution protection, the ONU has dual PON connections to two OLT PON ports (or two OLTs). When the protection group is configured to track the OLT's uplink Ethernet port, a Down state on that uplink is an OLT-side trigger. The OLT initiates the protection action (forces the working/standby role swap via PON protection signaling).
A - Correct behavior: After the OLT triggers protection, the ONU's working PON interface becomes standby, and the protect interface becomes working.
B - Correct behavior: The OLT monitors and updates the ONU uplink status as part of the protection group state machine.
C - Correct behavior: After inversion, services egress the ONU via the protect PON port toward the OLT, i.
e., traffic follows the configured protect path.
D - Incorrect (answer): In this scenario the trigger is the OLT's uplink Ethernet status, not an ONU-detected failure. Therefore the ONU does not detect the fault nor initiate the switchover; the OLT does.
(Reference: HCIP-Access V2.5 - GPON protection mechanisms; Huawei OLT protection group behavior, Type C dual-homing with uplink-tracking.)

NEW QUESTION: 33
(Radio) When the INVITE message sent by user A reaches user B after passing through servers C, D, and E, the Via header field entries recorded in the message received by user B appear in which order (top to bottom)?
A. C # D # E
B. E # C # D
C. E # D # C
D. C # E # D
Answer: (SHOW ANSWER)
In SIP, each proxy/server that forwards a request prepends its own address to the top of the Via header list.
Therefore, as A's INVITE traverses C, then D, then E, server E adds its Via at the top last, followed by D, then C below it. The message that reaches user B shows the Via stack (top#bottom) as E # D # C, which corresponds to option C. RFC 3261 states that the server transport uses "the value of the top Via header field" to determine response routing, confirming that the most recent hop is at the top

NEW QUESTION: 34
In video services, if the VOD service is normal but the live service encounters a black screen, which of the following are possible causes?
A. PQ is used for downstream congestion management of an OLT.
B. DWRR is used for upstream congestion management of an OLT.
C. On the ONU, the VLAN of the VoD service is different from that of the live service. On the OLT, there is only one video service stream.

D. The traffic profile corresponding to the OLT upstream multicast service flow is set to a low priority.

Answer: (SHOW ANSWER)

Live TV uses multicast, while VOD uses unicast. If VOD works but live TV is a black screen, typical causes are multicast service-path/config mismatches or priority starvation for multicast control/traffic:

C: If the ONU uses different VLANs for VOD and live but the OLT has only one video service flow, multicast frames will not match the correct service-port, causing black screen.

D: A low-priority traffic profile for multicast join/report or stream on the OLT uplink may drop IGMP joins or multicast packets under load, resulting in black screen while unicast VOD still passes.

Queue scheduling choices such as PQ or DWRR (A/B) are generic congestion schemes; by themselves they are not direct root causes of a live-only black screen unless mis-classified, whereas C and D are recognized multicast-specific fault points.

References: HCIP-Access V2.5 Study Guide - IPTV Multicast Service Flow, IGMP/Multicast QoS and Typical Faults (black screen with VLAN/service-port mismatch; priority of multicast control/stream).

NEW QUESTION: 35

The establishment, maintenance, and teardown of the signaling path between a SIP user and servers are done through an exchange of a series of SIP messages. Therefore, every piece of information in a SIP message is unique and no header information value ever appears multiple times.

A. wrong

B. Right

Answer: (SHOW ANSWER)

The statement is wrong. SIP explicitly allows several header fields to appear multiple times within a request or response-for example, Via (one per hop), Route, Record-Route, and Contact may legitimately occur more than once. This is fundamental to SIP routing behavior, where each proxy appends a new Via entry. RFC

3261 explains processing based on the top Via among potentially multiple Via headers, which directly contradicts the claim that "a single information value never appears multiple times

NEW QUESTION: 36

When the Type C dual-home protection linkage uplink detection is enabled, if the OLT or the OLT uplink fails, the Type C dual-home protection can switch over to another OLT.

A. True

B. False

Answer: (SHOW ANSWER)

Type C GPON protection uses two different OLTs (dual-home). With uplink status linkage configured, a failure of the active OLT itself or its uplink interface triggers a protection switchover to the standby OLT to maintain service continuity for ONUs homed through the protected ODN.

References: HCIP-Access V2.5 Study Guide (Type C Dual-Home Protection and Uplink Linkage); Huawei OLT Protection Feature Description (Type C Protection Behavior and Switchover Conditions).

NEW QUESTION: 37
In a campus project, XGS-PON is used; ONUs backhaul APs via a 1:16 splitter, but only 12 APs are actually connected per splitter. What is the downstream concurrent bandwidth per AP (Mbit/s)?
A. About 600
B. About 300
C. About 800
D. About 400
Answer: (SHOW ANSWER)
XGS-PON downstream line rate is ~10 Gbit/s. When 12 terminals share a PON tree concurrently, the rough per-terminal share is 10,000 Mbit/s ÷ 12 # 833 Mbit/s, commonly expressed as "about 800 Mbit/s." This aligns with planning examples in HCIP-Access where downstream concurrency on XGS-PON is calculated by dividing the port rate by the number of active ONUs/APs on the splitter.
References: HCIP-Access V2.5 Study Guide - PON Rate & Capacity Planning (XGS-PON 10G), Campus PON Design Examples - concurrency estimation.

NEW QUESTION: 38
When the H.248 protocol is used to deploy the VoIP service, the registration information sent by the MG to the MGC contains the following information:
Services {Method=Restart Reason=[901]}
Which command can trigger the information?
A. ONT re-register
B. Board restart
C. Reset coldstart
D. Reboot system
Answer: (SHOW ANSWER)
The MG reports availability and restarts to the MGC using H.248 ServiceChange with Method=Restart. The Reason code distinguishes the type of restart. In Huawei implementations aligned with H.248 semantics, Reason=[901] corresponds to a warm/warmboard restart scenario rather than a full cold start.
Board restart triggers a warm restart of the voice board/MG, producing ServiceChange { Method=Restart, Reason=901 }.
Reset coldstart performs a cold start, which would use a different reason code (cold start), not 901.
Reboot system generally implies a broader device reboot similar to cold start semantics, not 901.

ONT re-register affects ONU registration and does not cause the MG to announce a ServiceChange restart to the MGC.
References: HCIP-Access V2.5 Study Guide (H.248 ServiceChange usage and restart reporting); Huawei VoIP/MG Board Maintenance Guide (warm vs cold restart indications in ServiceChange).

NEW QUESTION: 39
The priority of the packets at the egress port can be mapped or set directly. Which of the following statements about priority processing is correct?
A. The priority policy must be tag-in-package regardless of the priority setting mode.
B. The priority mapping can be set separately for the inner and outer priorities.
C. The priority mapping needs to match the corresponding mapping profile. The mapping in a profile is fixed.
D. Priorities of outbound and inbound packets are strictly mapped. An outer VLAN ID cannot be mapped to the priority of an inner VLAN ID.
Answer: (SHOW ANSWER)
Huawei devices support independent mapping/remarking for inner and outer VLAN priorities (802.1p CoS) when QinQ is used. Operators can define distinct mapping tables or remark rules per tag. Option A is incorrect (priorities can be derived or remarked, not "must be" tag-in-packet), option C is incorrect because mapping profiles are configurable, and option D confuses VLAN IDs with priorities; inner/outer CoS can be mapped independently for inbound/outbound directions.
References: HCIP-Access V2.5 Study Guide (QoS Priority Mapping and Remarking); Huawei VLAN/QoS Configuration Guide (Inner/Outer 802.1p handling).

NEW QUESTION: 40
(Radio) 10G GPON system downlink wavelength is:
A. 1310 nm
B. 1577 nm
C. 1270 nm
D. 1490 nm
Answer: B (LEAVE A REPLY)
In Huawei's 10G GPON (Gigabit-capable Passive Optical Network) system, different optical wavelengths are used for upstream and downstream transmission to ensure bidirectional communication over a single fiber.
According to the ITU-T G.987.x series and Huawei's Access Network Technical Documentation, the wavelength plan for 10G GPON (XG-PON) is as follows:
Downstream (OLT # ONU): 1577 nm
Upstream (ONU # OLT): 1270 nm
This separation of wavelengths allows both transmission directions to occur simultaneously using WDM (Wavelength Division Multiplexing) on the same optical fiber, minimizing interference.

Huawei OLTs such as the MA5800 and EA5800 series follow this standard exactly - supporting 10G GPON (XG-PON) with downstream at 1577 nm and upstream at 1270 nm.Hence, the correct answer is 1577 nm.
References (Aligned with HCIP-Access V2.5 and Huawei Technical Sources):
HCIP-Access V2.5 Study Guide - "Huawei Campus Network Overview" Chapter, Section: PON Technology Overview Huawei 10G GPON (XG-PON) Technical White Paper ITU-T G.987.2: 10-Gigabit-capable Passive Optical Networks (XG-PON): Physical Media Dependent (PMD) Layer Specification Huawei MA5800 Product Description - 10G GPON Port Wavelength Specifications

NEW QUESTION: 41
Under the H.248 protocol, if the signaling IP and media IP are both 10.1.1.100/8, and the voice gateway is
10.1.1.1, when configuring VoIP service, which command is incorrect?
A. Using the command ip address media 10.1.1.100 10.1.1.1 in voip view to configure the media IP
B. Use the reset coldstart command under the H.248 interface so interface property configuration takes effect
C. Use the if-h248 attribute command to configure interface properties under the H.248 voice interface
D. Using the command ip address signaling 10.1.1.100 10.1.1.1 in voip view to configure the signaling IP
Answer: (SHOW ANSWER)
On Huawei access devices/OLTs, VoIP/H.248 setup typically includes:
In voip view, configure media IP with gateway:
ip address media <media-ip> <gateway> - e.g., ip address media 10.10.10.10 10.10.10.1.
Configure signaling IP without a gateway parameter:
ip address signaling <signaling-ip> - e.g., ip address signaling 10.10.10.10.
Add/enter the H.248 interface and apply properties with if-h248 attribute ....
It's common to reset/enable the MG interface after attribute changes; many guides show reset coldstart (or reset) issued under the H.248 interface to activate the interface.
Authoritative configuration examples show media takes an IP and gateway, but signaling takes only the IP.
Therefore, option D (attempting to configure signaling with a gateway parameter) is incorrect.
Options A and C match documented syntax and workflow. Option B reflects the documented practice of issuing a reset (often written as reset coldstart) under the H.248 interface to apply/enable, as shown in Huawei-focused configuration guides.

NEW QUESTION: 42
The maximum spectroscopic (split) ratio supported by 10G EPON is?
A. 1:256 (Laboratory)
B. 1:32

C. 1:128
D. 1:64
Answer: (SHOW ANSWER)
In HCIP-Access teaching materials, 10G-EPON improves optical budget and FEC efficiency compared with
1G EPON, enabling very high split ratios. While commercial deployments commonly use 1:64 or 1:128 depending on optics class and reach, the maximum (laboratory) split ratio often cited for the technology is 1:
256 under favorable conditions.
References: HCIP-Access V2.5 Study Guide - 10G-EPON capabilities (rates, optics classes, and maximum
/theoretical split ratios).

NEW QUESTION: 43
In eSight's ONT zero-configuration (zero-touch) deployment, do not provision the OLT when incrementally configuring the OLT.
A. True
B. False
Answer: (SHOW ANSWER)
For ONT zero-touch on eSight/iMaster NCE-Campus, the prerequisite is that the OLT is onboarded and provisioned (communication parameters, northbound credentials, templates) so that discovered ONTs can inherit policies and be auto-activated. During incremental OLT configuration, eSight does push/update the OLT's configuration (templates, profiles, authentication rules). Saying "do not provision OLT" is therefore false.
References: HCIP-Access V2.5 Study Guide - Network Management & Maintenance (ONT Zero-Touch workflow and OLT prerequisites); eSight ONT Zero-Touch Deployment Guide - Incremental OLT configuration and template delivery.

NEW QUESTION: 44
On Network Cloud Engine (NCE), both manual dump and automatic dump allow you to dump the performance data that meets the criteria to a file on the local disk.
A. TRUE
B. FALSE
Answer: (SHOW ANSWER)
NCE supports on-demand (manual) and policy-driven (automatic) performance data dumps. In both modes, data filtered by configured criteria is exported to files stored locally on the NCE server for subsequent analysis or archiving.

NEW QUESTION: 45
If the ONT zero touch provisioning function is enabled on the eSight, the OLT does not need to be preset during incremental configuration.

A. TRUE
B. FALSE
Answer: (SHOW ANSWER)
With ONT Zero-Touch Provisioning (ZTP) enabled on eSight, newly discovered ONTs can be automatically identified and provisioned by pushing service templates from eSight. This removes the need for advance (preset) service configuration on the OLT during incremental onboarding; the OLT simply accepts the provisioning delivered by eSight.

NEW QUESTION: 46
Deploying an Ethernet port protection group in the upstream direction of the OLT can improve the reliability and the bandwidth of the uplink.
A. TRUE
B. FALSE
Answer: (SHOW ANSWER)
An Ethernet port protection group is a 1:1 protection mechanism that improves reliability through active
/standby switching. It does not aggregate bandwidth-the standby port does not forward traffic unless a switchover occurs. If increased bandwidth is required, technologies such as LACP are used instead.
References: HCIP-Access V2.5 - Uplink Protection vs. Link Aggregation; OLT Ethernet Port Protection Group Feature Description.

NEW QUESTION: 47
In the upstream direction of the OLT, link aggregation can be used to improve bandwidth and reliability.
Which OLT uplink aggregation modes are supported?
A. Automatic
B. Manual
C. Static
D. Dynamic
Answer: (SHOW ANSWER)

Huawei OLTs support Eth-Trunk (link aggregation) with two standard modes: Static aggregation and Dynamic aggregation (LACP). These provide bandwidth expansion and redundancy on NNI uplinks.
"Automatic" is not a defined mode; and "manual" is not used as a separate mode name in OLT Eth-Trunk configuration.
References: HCIP-Access V2.5 Study Guide - OLT Uplink Design (Eth-Trunk), OLT Interface Configuration - Static vs LACP (Dynamic) aggregation.

NEW QUESTION: 48
(Radio) When configuring multicast services on MA5600T/MA5680T, the programs of multicast VLANs are statically configured. Which of the following must be configured, otherwise the multicast programs may not be able to be watched?
A. igmp profile
B. igmp program
C. igmp priority
D. igmp preview
Answer: (SHOW ANSWER)
On Huawei OLTs (e.g., MA5600T/MA5680T), deploying IPTV/multicast commonly uses a program list (channel list) to map program numbers to multicast group addresses-this is configured with igmp program.
When programs are statically configured under the multicast VLAN, the program definitions themselves are mandatory; without them, set-top boxes cannot select (zap to) channels by program number/address mapping and the OLT cannot correctly forward the requested multicast streams.

NEW QUESTION: 49
Layer 2 enables IGMP Snooping, and when the switch port receives an IGMP Join (Membership Report), it listens to the packet and adds the corresponding port to the multicast group.
A. wrong
B. Right
Answer: B (LEAVE A REPLY)
IGMP Snooping is a Layer-2 function that listens to IGMP control packets between hosts and the multicast querier. Upon receiving a host's Membership Report (Join) for group G, the switch learns that the ingress port is a member port for G and adds that port to the group's forwarding entry, so multicast traffic for G is forwarded only to those learned member ports (saving bandwidth and avoiding flooding). Huawei's official documentation describes IGMP Snooping exactly in this way.

NEW QUESTION: 50
The protection scope of GPON Type B dual-homing protection covers ( ).
A. Active and standby backbone optical fibers

B. Active and standby OLTs
C. Active and standby PON ports of the OLT
D. Active and standby branch optical fibers
Answer: (SHOW ANSWER)
Type B provides redundancy with two OLT PON ports on the same OLT and two feeder (backbone) fibers to the ODN. Therefore it protects the PON ports and the backbone/feeder path. It does not protect the OLT itself (still a single OLT) and does not protect the ONU branch fibers.
References: HCIP-Access V2.5 Study Guide - PON Line Protection Scope (Type B: OLT port + feeder fiber; no branch/OLT equipment protection).

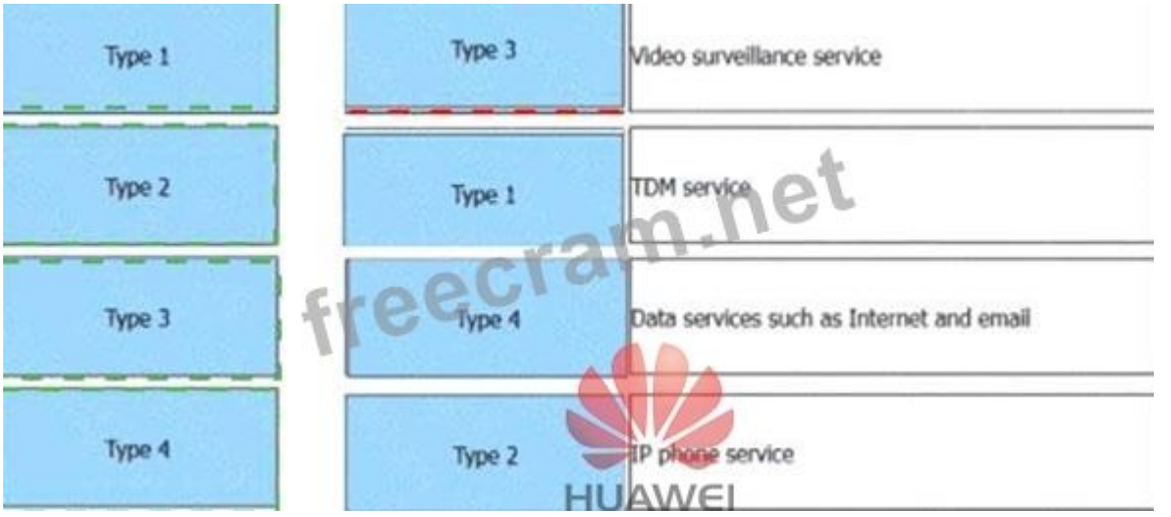
NEW QUESTION: 51
When the DHCP Option 82 function is enabled globally and in the VLAN service profile and the port/service- port is configured to allow user-side DHCP packets to carry Option 82, what is the processing policy if a user- side DHCP packet already containing Option 82 is received?
A. The access device strips the Option 82 information from the user-side DHCP packet and forwards the packet.
B. The access device directly forwards the user-side DHCP packet without any processing.
C. The access device strips the Option 82 from the user-side DHCP packet and adds the local user information.
D. The access device discards the user-side DHCP packet.
Answer: (SHOW ANSWER)
In Huawei access network devices (such as MA5800, EA5800, and SmartAX series), the DHCP Option 82 (Relay Agent Information Option) feature is used to identify the source location of DHCP requests coming from users connected to access ports.
This helps the DHCP server assign IP addresses based on access topology information, such as slot, port, and VLAN IDs.
When Option 82 is enabled globally and within the VLAN service profile, and the port/service-port is configured to allow user-side packets to carry Option 82, the device processes incoming DHCP requests as follows:
* If a user-side DHCP packet does not contain Option 82:# The device automatically adds local Option
82 information (e.g., circuit ID, remote ID) before forwarding it to the DHCP server.
* If a user-side DHCP packet already contains Option 82:# The device removes (strips) the existing Option 82 field to prevent spoofing or inconsistent location data.# Then it adds its own local Option 82 information (accurate relay agent data based on the device's configuration).# The modified packet is then forwarded to the DHCP server.
This ensures that only trusted network-side Option 82 data is passed along, maintaining accurate user-location binding for IP address management and security.
Therefore, the correct behavior is:
The access device strips the Option 82 field from the user packet and adds its own local Option 82 information.

References (Aligned with HCIP-Access V2.5 and Huawei Technical Documents):
* HCIP-Access V2.5 Study Guide - "Huawei Campus Network Overview" Chapter, Section: DHCP Relay and Option 82 Mechanism
* Huawei MA5800/EA5800 Configuration Guide - IP Service # DHCP Relay and Option 82 Configuration
* Huawei Enterprise Networking Product Documentation: "Understanding DHCP Option 82 Processing"
* Huawei Access Network Feature Guide, Section: Processing Policies of DHCP Packets with Option 82

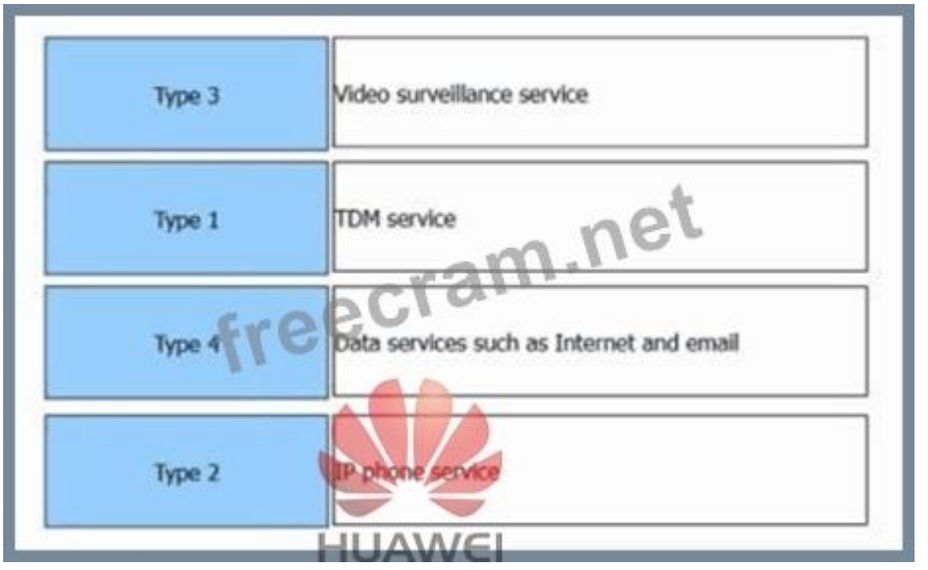
NEW QUESTION: 52
During troubleshooting, you can obtain multiple requests and response messages in a session by capturing packets. Which of the following options can be used to confirm the mapping between requests and response packets?
A. Branch ID
B. From
C. CSeq
D. Tag
Answer: (SHOW ANSWER)
In SIP message correlation, a response matches a request using the CSeq header (method and sequence number) together with the dialog identifiers (Call-ID, From/To with tags). Among the options, CSeq is the direct, standard field used to pair a specific request with its corresponding response within the same dialog.
References: HCIP-Access V2.5 (SIP message structure and troubleshooting: CSeq-based mapping of requests
/responses).

NEW QUESTION: 53
Different DBA need to be configured for different services. Drag the DBA to corresponding services. (Score only when all the answers are correct.)

Answer:



Explanation:



NEW QUESTION: 54

In Huawei U2000, when adding network elements, you can only add them one-by-one while accessing each network element.

A. Wrong

B. Right

Answer: (SHOW ANSWER)

This statement is wrong. In U2000, network elements (NEs) can be added by multiple methods, including batch addition/import and automatic discovery, not just one-by-one during a live access session. U2000 supports template-based onboarding and batch operations to improve efficiency for large-scale deployments.

References: HCIP-Access V2.5-Network Management chapter (U2000 NE addition methods, discovery, and batch import); Huawei U2000 Administrator Guide (NE management and batch operations).

NEW QUESTION: 55

Sequence of upstream QoS processing on the OLT:

A. Traffic classification > Marking > ACL policy > Congestion avoidance > Congestion management

B. Marking > Traffic classification > Congestion avoidance > Traffic policing > Congestion management

C. Traffic classification > Marking > Congestion avoidance > Traffic policing > Congestion management

D. Traffic classification > Marking > Traffic policing > Congestion avoidance > Congestion management

Answer: (SHOW ANSWER)

On Huawei OLTs, the standard QoS pipeline for upstream packets is: first perform traffic classification (identify flows), then marking (set CoS/DSCP as required), next apply traffic policing (rate-limit and color traffic), followed by congestion avoidance (AQM such as RED/WRED), and finally congestion management (queue scheduling/priority queuing). This ordered sequence ensures correct identification and marking before any rate enforcement, and that packets encounter AQM prior to scheduler-based dequeue.

Reference: HCIP-Access V2.5 - QoS Framework and Processing Sequence on OLT (classification # marking
policing # AQM # scheduling).

NEW QUESTION: 56

In the evolution from EPON to 10G-EPON, a smooth transition is achieved at the central office by adding WDM modules, and ODNs can coexist/reuse.

A. True

B. False

Answer: (SHOW ANSWER)

IEEE 802.3av (10G-EPON) explicitly enables coexistence of 1G-EPON and 10G-EPON on the same outside plant (ODN) by separating downstream wavelengths (1G ~1480-1500 nm vs 10G ~1575-1580 nm) and using dual-rate TDMA in the upstream (10G uses 1260-1280 nm within the broader 1G band). This wavelength plan and OLT capabilities allow operators to reuse existing

ODN and achieve a smooth upgrade via WDM overlays at the OLT. Industry and standards materials emphasize this approach for incremental migration.