DUMPSARENA

Alcatel-Lucent Advanced Troubleshooting

Alcatel-Lucent 4A0-110

Version Demo

Total Demo Questions: 6

Total Premium Questions: 60

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

An LDP targeted session between two routers does not establish. Which of the following should be verified during troubleshooting? Select three answers.

A. Reachability to the remote LDP transport address

B. TCP port 646 filtering

C. Targeted-peer configuration on both routers

D. Ethernet multicast forwarding on the path

E. RSVP reservable bandwidth

ANSWER: A B C

Explanation:

An LDP targeted session is established over TCP using the LDP transport address, rather than requiring the routers to be directly connected. The configured targeted peer address must therefore be reachable in the routing table. TCP connectivity to port 646 must also be permitted in both directions; an ACL or filter that blocks TCP port 646 prevents session establishment. Finally, both routers must have compatible targeted-session configuration so that each router accepts or initiates the intended targeted LDP relationship.

Link-layer multicast operation is relevant to basic LDP discovery on directly connected interfaces, but it is not required for the targeted TCP session itself. RSVP bandwidth reservation is also independent of LDP targeted-session establishment. LDP session establishment and targeted discovery are defined in RFC 5036. Nokia SR OS MPLS and LDP configuration guidance is available through the Nokia SR OS documentation portal.

QUESTION NO: 2

The mesh-sdp binding for a VPLS configured on Node 1 is down with an error

serviceMTUMismatch. One sap is configured in the VPLS and it is up with default mtu 1514. The LDP binding display on Node 1 shows that there is a mismatch on the MTU value. What are the required configurations on Node 1 to bring the VPLS up?

Node 1

```
config>service>
        vpls 200
           sap 1/1/5 create
           exit
           spoke-sdp 43:200 create
           exit
           no shutdown

# show router ldp bindings
===============================================================================
LDP Service Bindings
===============================================================================
Type   VCId     SvcId    SDPId  Peer            IngLbl  EgrLbl  LMTU  RMTU
-------------------------------------------------------------------------------
V-Eth  200      200      43     10.10.1.3       131071U 131070  1500  9176
```

A. Set the sap port mtu to 9176

B. Set the service-mtu to 9176

C. Set the service-mtu to 9190

D. Set the sap port mtu to 9190

E. Set the service-mtu to 1514

ANSWER: B D

Explanation:

Set the service-mtu to 9176 and set the sap port mtu to 9190. In SR OS Ethernet services, the service MTU represents the maximum customer Ethernet frame handled by the service, while the Ethernet port MTU must also accommodate the 14-byte Ethernet MAC header. Consequently, a 9190-byte port MTU supports a maximum service MTU of 9176 bytes. These values align the local VPLS service MTU with the MTU advertised through the LDP mesh-SDP binding and remove the `serviceMTUMismatch` condition. The SAP's current default 1514-byte service capability is insufficient when the far-end VPLS binding advertises the jumbo service MTU shown in the binding information. Both the service-level setting and the underlying SAP port capability must be configured consistently: changing only the service value would leave the port unable to carry the required frame size, while changing only the port would leave the VPLS signaling MTU unchanged. Once the VPLS service is configured for 9176 and its SAP port is configured for 9190, the MTU advertised and accepted for the mesh SDP can match, allowing the pseudowire binding to become operational. Nokia's SR OS documentation describes Ethernet service MTU and port-MTU relationships in its Services Overview Guide and provides related configuration context in the Layer 2 Services Guide.

QUESTION NO: 3

An operator has entered the following CLI commands to configured redistribution of OSPF routes into ISIS. None of the active OSPF routes are redistributed into ISIS, what is the problem in the CLI commands?

```
config>router>policy-options> begin
        policy-statement ospf-isis
            entry 10
                action accept
                from
                    protocol ospf
                exit all
config>router>isis>
        area-id 69.1000
        export "ospf-isis"
        interface "toNode2"
```

A. OSPF area has to be configured as NSSA

B. Default-action has to be configured as accept

C. Import policy has to be configured under OSPF

D. The policy is still in edit mode, therefore it will not take any effect

E. to protocol isis has to be added under entry 10

ANSWER: D

Explanation:

The policy is still in edit mode, therefore it will not take any effect. In the SR OS classic CLI workflow, a configuration session started with `begin` is a candidate edit session. The policy entries, route match conditions, and accept action can be syntactically correct, but they are not applied to the active/running configuration until the operator exits the edit process appropriately and commits the candidate configuration. Consequently, the IS-IS export policy does not yet have an active policy statement from which it can accept OSPF-learned routes for redistribution.

After validating the policy content, the operator must use `commit` so that the pending configuration becomes operational. Once committed, the configured export policy can evaluate active OSPF routes and export the routes that match its terms into IS-IS. This behavior is intentional: the candidate configuration model allows related changes to be made and reviewed as a single transaction before they affect routing behavior. Nokia's SR OS documentation provides the authoritative CLI and configuration-management guidance at Nokia Documentation Center and in the SR OS documentation library.

QUESTION NO: 4

A policy is configured to redistribute four active static routes into ISIS. No ISIS route is received on the far end, what is the cause of the problem?

```
config>router>policy-options>
        policy-statement static-isis
            entry 10
                from
                    protocol static
config>router>isis>
        area-id 69.1000
        export "static-isis"
        interface "toNode2"
```

A. Action accept?has to be configured for entry 10

B. Default-action has to be configured as accept

C. Import policy should be configured under ISIS instead of export policy

D. Within entry 10, to protocol isis has to be configured

E. A prefix list has to be configured to filter the routes

ANSWER: A

Explanation:

Action accept has to be configured for entry 10 is correct. In SR OS routing policy processing, matching a route against the `from protocol static` condition does not itself authorize redistribution. The matching policy entry must specify a disposition action that accepts the route. An `action accept` terminates policy evaluation for that route and permits it to be exported by the IS-IS protocol policy. Without this action, the matching static routes are not accepted for advertisement; if the policy's default behavior is reject, they are consequently suppressed and the remote IS-IS router receives no routes.

This is especially important when a policy is used as an IS-IS export policy: the policy controls which routes from the local routing table may be injected into IS-IS, and an explicit accepting action is the normal, deterministic configuration for selected redistributed prefixes. Once entry 10 both matches the active static routes and accepts them, IS-IS can create the appropriate external reachability advertisements, subject to normal IS-IS adjacency and level configuration. Nokia's SR OS documentation describes routing-policy entries as match conditions combined with actions and documents their use by routing protocols: Nokia SR OS Routing Policies and Nokia SR OS IS-IS documentation.

QUESTION NO: 5

What are the possible logging destinations supported on the Alcatel 7x50?

A. Syslog

B. Session

C. FTP server

D. Memory log

E. Compact flash

ANSWER: A B D E

Explanation:

On Alcatel-Lucent 7x50 routers running SR OS, event-log policy identifies a destination to which matching log events are written. **Syslog** is supported for forwarding event messages to a configured remote syslog collector, allowing centralized operational monitoring and retention. **Session** is a supported destination for presenting selected event messages to an active management session, which is useful while an operator is connected and troubleshooting. **Memory log** is also supported: SR OS maintains log entries in an in-memory buffer for local inspection with operational show commands. Finally, **Compact flash** represents the SR OS file logging destination. A log file can be written to the router's compact-flash file system, providing persistent local storage that remains available after an event has aged out of memory or the router is restarted. These destinations are configured under the SR OS logging and event-control framework, where one or more log IDs and filters determine which events are sent to each destination. Nokia's SR OS system-management documentation

describes the supported logging framework and destination behavior in its Logging documentation; the broader SR OS documentation library is available at Nokia Documentation.

QUESTION NO: 6

What MPLS tunnel label(s) will be used in the data packet traveling on LSP toR4 FRR leaving from Node 3 to Node 4?

Node 3

```
# show router mpls lsp toR4FRR path detail

===============================================================================
MPLS LSP toR4FRR Path  (Detail)
===============================================================================
Legend :
    @ - Detour Available              # - Detour In Use
    b - Bandwidth Protected           n - Node Protected
===============================================================================
-------------------------------------------------------------------------------
LSP toR4FRR Path toPod4
-------------------------------------------------------------------------------
LSP Name     : toR4FRR                          Path LSP ID      : 17
From         : 10.10.1.3                        To               : 10.10.1.4
Adm State    : Up                               Oper State       : Up
Path Name    : toPod4                           Path Type        : Primary
Path Admin   : Up                               Path Oper        : Up
OutInterface: n/a                               Out Label        : n/a
Path Up Time: 0d 00:06:15                       Path Dn Time     : 0d 00:00:00
Retry Limit : 0                                 Retry Timer      : 30 sec
RetryAttempt: 3                                 Next Retry In    : 6 sec
Bandwidth    : No Reservation                   Oper Bandwidth   : 0 Mbps
Hop Limit    : 255
Record Route: Record                            Record Label     : Record
Oper MTU     : 9198                             Negotiated MTU   : 9198
Adaptive     : Enabled                          MBB State        : N/A
Include Grps:                                   Exclude Grps     :
None                                            None
Path Trans   : 19                               CSPF Queries     : 6
Failure Code: badNode                           Failure Node     : 10.1.5.1
ExplicitHops:
    10.10.1.4
Actual Hops :
    10.1.5.2(10.10.1.3) @ #
 -> 10.1.4.2(10.10.1.4)                         Record Label     : 131068
===============================================================================

# show router mpls bypass-tunnel

===============================================================================
MPLS Bypass Tunnels
===============================================================================
To              State   Out I/F       Out Label     Reserved     Protected
                                                    BW (Kbps)    LSP Count
-------------------------------------------------------------------------------
10.1.4.2        Active  1/1/6         131069        0            2
-------------------------------------------------------------------------------
Bypass Tunnels : 1
```

A. 131069 131068

B. 131068 3

C. 131069

D. 131068

E. No label is used in the data packet

ANSWER: A

Explanation:

The data packet sent from Node 3 toward Node 4 on the protected *toR4 FRR* LSP carries the label stack **131069 131068**. Label 131068 is the RSVP-TE transport label associated with the original LSP forwarding state. During fast reroute operation, Node 3 must also direct traffic through the locally selected protection tunnel. It therefore pushes the additional, outer label 131069, which identifies the FRR bypass or detour forwarding context. MPLS forwarding always processes the top label first, so the next hop uses 131069 to follow the protection path; the inner 131068 remains intact so that, when the repair path rejoins the protected LSP, forwarding can continue according to the original LSP state. This label stacking is the essential RSVP-TE FRR behavior: the backup tunnel is imposed locally without requiring ingress re-signaling or changing the original LSP label carried by the packet. Nokia's MPLS documentation describes RSVP-TE LSP label operations and protection behavior in its MPLS guide; RFC 4090 defines the RSVP-TE fast-reroute mechanisms, including bypass and detour tunnels, at RFC 4090.