Product Notice #0221

Guidelines for Mediant MSBR Deployments with SBC or CRP Functionality

Notice Subject

This notice highlights important considerations when deploying the Mediant MSBR in a network with an E-SBC or Cloud Resiliency Package (CRP) license.

Notice Date

October 6th, 2014

Notice Effective Date

Immediate

Affected Product Family

- MSBR series

Notice Details

While the Mediant MSBR series supports SBC and CRP functionality for a hosted and SIP Trunking environment, its network architecture significantly differs from the AudioCodes E-SBC product family. The key differences relate to the data-routing capabilities, which are available in the Mediant MSBR series but unavailable in the E-SBC series.

AudioCodes Inc.
27 World's Fair Drive, Somerset, NJ 08873
Tel: +1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
1 Hayarden Street, Airport City, Lod 7019900
P.O. Box 255, Ben Gurion Airport, Israel, 7019900
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
www.audiocodes.com/info
Website: www.audiocodes.com

The table below lists the topics that should be considered whenever a Mediant MSBR with SBC or CRP functionality is deployed in the network.

Functionality	Mediant MSBR with SBC/CRP and Data Routing	Mediant MSBR with SBC/CRP without Data Routing
Forwarding mode	• The MSBR is a router with SBC capabilities. Its routing engine routes not only voice, but also all TCP/UDP traffic. • LAN ports are switched Ethernet interfaces. • WAN ports are routed interfaces.	• The SBC forwards only voice traffic. • Ethernet ports are separate interfaces (pair or dedicated modes).
Secured connectivity to untrusted networks	Connect the MSBR to untrusted or public IP networks through either of its WAN ports (number and type of WAN ports are model dependent) and activate the firewall functionality (see below).	Either of the SBC Ethernet ports can be connected to untrusted or public networks.
Firewall	• Stateful Packet Inspection Firewall should be activated on the MSBR WAN interface/s. The firewall dynamically opens pinholes for LAN-initiated connections. WAN-initiated connections are dropped. • ACLs can be applied to MSBR interfaces to permit/drop an unwanted traffic type, thereby overruling the firewall. • No need to configure ACLs on voice interfaces.	The SBC dynamically opens pinholes for established calls. All traffic other than voice is blocked.
VLANs	• Configured on either or both LAN and WAN interfaces. • VLAN usually represents the layer 3 subnet; packets are routed from one VLAN to another, unless ACLs or Firewall are invoked (as described above).	• Configured on voice network interfaces. • There is no layer 3 routing between interfaces or VLANs. SBC logic determines how to forward voice packets between VLANs.

Functionality	Mediant MSBR with SBC/CRP and Data Routing	Mediant MSBR with SBC/CRP without Data Routing
OAM&P	• Available by default through any of the configured IP interfaces, including loopback interfaces, LAN interfaces, VLAN interfaces and logical interfaces (e.g. Tunnel interfaces). • OAM&P authorization can be restricted by ACLs.	• Available through a dedicated OAM&P interface.