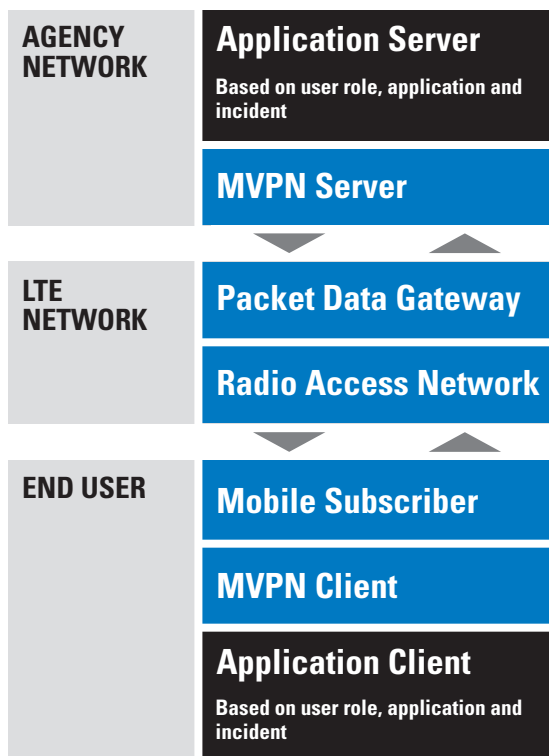




PUBLIC SAFETY LTE DESIGN CRITICAL CONSIDERATIONS FOR USING QoS WITH MVPN

OVERVIEW

Next Generation Public Safety networks will be used by multiple groups that often have unique needs and missions. For example, first responders need urgent access to information in life and death situations while public service workers need transactional data to do their daily job better. Each agency will have a wide variety of applications in use on the network, and each application will have different requirements which can change depending on user role and mission.



Long Term Evolution (LTE) is the next generation in IP wireless networks providing higher capacity and speeds to support high bandwidth applications such as video streaming. Even with the higher capacity and speeds, there will be situations when the local user demand is greater than what the network can supply. This is when public safety networks will need to prioritize users and applications to meet the mission requirements.

Public safety agencies often use Mobile Virtual Private Networks, or MVPN, on existing wireless data networks to protect sensitive data as it travels across various IP networks. To ensure satisfactory results when implementing prioritization controls such as Quality of Service (QoS), it is important to understand the interaction of QoS and MVPN.

QUALITY OF SERVICE

Quality of Service, or QoS, is a method to identify and provide a differentiated level of service. On a Public Safety LTE system, the ability to dynamically assign QoS allows the system to prioritize data flows based on the application and agency policies.

Differentiated Services, or DiffServ, is a computer networking architecture that specifies a mechanism for classifying and managing network traffic and providing Quality of Service guarantees on IP networks. The relative importance of each IP packet is specified using the Differentiated Services Code Point (DSCP) field in the IP header. Reference RFC 2474 for more information.

Motorola's Public Safety LTE network supports the selection of QoS policy based on the DSCP marking of the bearer traffic.

QoS AND MVPN

Public safety customers often utilize a Mobile Virtual Private Network for security and mobility. The introduction of a MVPN can have a bearing on differentiated quality of service. A MVPN creates a secure tunnel between the agency and the mobile client. User data is encrypted and encapsulated within an IP tunnel, and information traveling within this secure tunnel is not visible to any device external to the tunnel.

This lack of visibility can create issues with DiffServ QoS architectures; because the IP network cannot penetrate the tunnel, it cannot retrieve the DSCP marking in the IP header and cannot act on the QoS policies. To enable proper operation of dynamic Quality of Service, the MVPN must copy the DSCP field of the original application traffic to the outside of the MVPN IP packet. This enables downstream network elements to execute the QoS policies specified by the application or the requesting agency.

Some MVPNs support static configurations of QoS policy for application data within the MVPN itself. However, static configuration is not sufficient to address the dynamic nature of the public safety user. For mission-critical applications, the importance of a particular application and/or user will change based on the critical nature of the particular mission. As a result, marking the packets external to the MVPN is the only way to dynamically execute QoS.

As discussed earlier, the MVPN needs to provide DSCP marking external to the secure tunnel for QoS operation. During this process, all traffic bundled in the same tunnel will be externally marked at the same QoS level causing the network to provide the same QoS treatment. If the bundle contains traffic of different QoS levels, it will then be mismarked external to the tunnel, resulting in the incorrect priority treatment. To avoid this, the MVPN should not bundle traffic of different QoS levels within the same tunnel.

CONCLUSION

Understanding the interaction of QoS and MVPNs is critical for proper operation. The transparent passing of application-sourced DSCP allows for accurate prioritization within Next Generation Public Safety LTE networks. Allowing the application traffic to be uniquely tunneled, unbundled with other application traffic, allows proper public safety QoS treatment. The selection of a MVPN product with compatible public safety QoS features is imperative to meet the demands of mission critical data environments.

NEXT GENERATION PUBLIC SAFETY

At the heart of every mission is the ability to communicate in an instant to coordinate response and protect lives. Today, Motorola is putting real-time information in the hands of mission critical users to provide better outcomes.

Our powerful combination of next generation technologies is transforming public safety operations by strengthening the mission critical core with broadband connections, rich-media applications, collaborative devices and robust services. It's Technology That's Second Nature™.

To find out more, visit motorolasolutions.com/nextgen.

Motorola, Inc. 1301 E. Algonquin Road, Schaumburg, Illinois 60196 U.S.A. motorolasolutions.com

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2011 Motorola Solutions, Inc. All rights reserved. G4-36-101

