Network Management Practices

Sebastian participates in standard network management practices and does not discriminate against any form of traffic for any reason. The following sections provide a detailed explanation of Sebastian's network practices:

Blocking

Sebastian does not block any lawful traffic, services, or applications that would affect end-users. This ensures that users have unrestricted access to all legal content and services available on the internet without any restrictions imposed by the network.

Throttling

Sebastian does not engage in any form of throttling that would impede the end-user experience based on the type of traffic, content, service, or user. This commitment guarantees that all data gets treated equally, providing a consistent and reliable internet experience for all users.

Traffic Prioritization

Sebastian does not prioritize traffic through traffic shaping, prioritization, or resource reservation for the benefit of an affiliate. All traffic is managed equally, ensuring a fair and unbiased distribution of network resources.

Paid Prioritization

Sebastian does not engage in paid prioritization, meaning no traffic gets favored through traffic shaping, prioritization, or resource reservation in exchange for monetary or other considerations. This practice ensures that all users have equal access to the network.

Congestion Management

Sebastian employs standard congestion management protocols to maintain network performance and reliability. Techniques such as network redundancy are used to manage all types of traffic traversing Sebastian's network, ensuring a smooth and uninterrupted user experience even during peak usage times.

Application-Specific Behavior

Sebastian does not block or rate-control any ports or protocols, nor does it modify protocol fields outside of the protocol standard. Furthermore, Sebastian does not favor any applications over others, maintaining a neutral stance towards all internet applications and services.

Device Attachment Rules

Sebastian does not restrict the type of device an end-user can connect to its network, provided the device is UL and FCC certified. This ensures that users can connect a wide range of devices without any unnecessary limitations.

Security

Sebastian employs multiple network security practices to ensure end-user security in accordance with network management standards. These practices include:

- **DHCP Services:** Dynamic Host Configuration Protocol services to manage IP address allocation securely.
- **MAC Limits:** Media Access Control to limit the number of IP Addresses Subscribers can connect to the network and enhance security.
- **DDoS Monitoring:** Continuous monitoring for Distributed Denial of Service attacks to protect the network and its users from malicious activities.

Machine Readable Broadband Labels

All machine-readable broadband labels are viewable at http://sebastiancorp.com/MRL