

Business Class Hotspots with L2TP



While users enjoy the proliferation of Wi-Fi in hotspots, the distributed nature of these locations can cause problems for broadband providers.

First, providers must deliver consistent access policies and user experience across all locations. This may include various authentication schemes, a selection of free services, and a user interface that protects the provider's brand name while allowing for delivery of dynamic content.

The management overhead of updating policies across distributed access points can be costly and is often error prone.

Second, service providers are obligated to monitor and restrict user activity in order to prevent malicious use of the network.

This includes restrictions on outgoing and incoming traffic to prevent attackers from using the network.

With major concerns around terrorists and criminals using the Internet, service providers may be subpoenaed to monitor and report specific user activities, according to CALEA requirements.

Ruckus Wireless has solved these problems by implementing transparent bridging through the use of L2TP tunnelling. By tunnelling traffic from a Ruckus AP to a centralized data center, access controllers with policy enforcement software apply rules and services in a cost-effective manner. In a typical hotspot implementation these rules include a captive portal to authenticate users' credentials.

FEATURES/BENEFITS

- L2TP tunnel bridges Wi-Fi clients onto carrier network
- Ethernet packets tunneled using BCP/PPP/L2TP
- MAC addresses visible to broadband provider allowing device authentication
- Consistent access policies and user experience everywhere
- Monitor and restrict user activity to prevent malicious use of network
- IP addresses can be allocated by centralized DHCP server
- Ability to transport VLAN tags allows different policies to be applied to each SSID
- Single L2TP tunnel simplifies operation and management overhead
- QoS policies enforced at the edge to maximize performance and enable multimedia services

SUPPORTED RFCs

- RFC 1661 — PPP
- RFC 2661 — L2TP
- RFC 3518 — PPP/BCP



