

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.

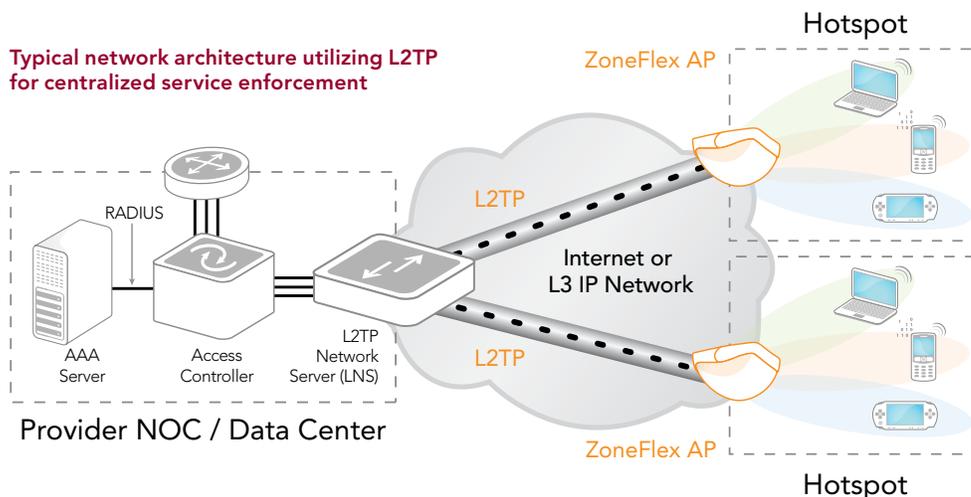
Ruckus Wireless has solved these problems by implementing transparent bridging through the use of L2TP tunnelling. By tunnelling traffic from a Ruckus AP to a centralized data center, access controllers with policy enforcement software apply rules and services in a cost-effective manner. In a typical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



This same architecture is extensively used at the edge of wired networks by providers offering Internet connections to subscribers using broadband access technology.

Commercially proven L2TP Network Servers (LNS), devices that aggregate and terminate tunnels at the core of the network, are widely available to address the need of small networks with only few hundred tunnels and very large networks with hundreds of thousands of tunnels.

In some cases, vendors have integrated the LNS functionality within access controllers, particularly for large scale networks. The L2TP tunnel also provides great flexibility in terms of network topology as the tunnel may traverse any Layer-3 network, including the Internet.

The Ruckus AP uniquely functions as a remote bridge. As such, it forwards traffic into PPP sessions over the L2TP (Layer 2 Tunneling Protocol) tunnel, using the Bridge Control Protocol (RC-3518).

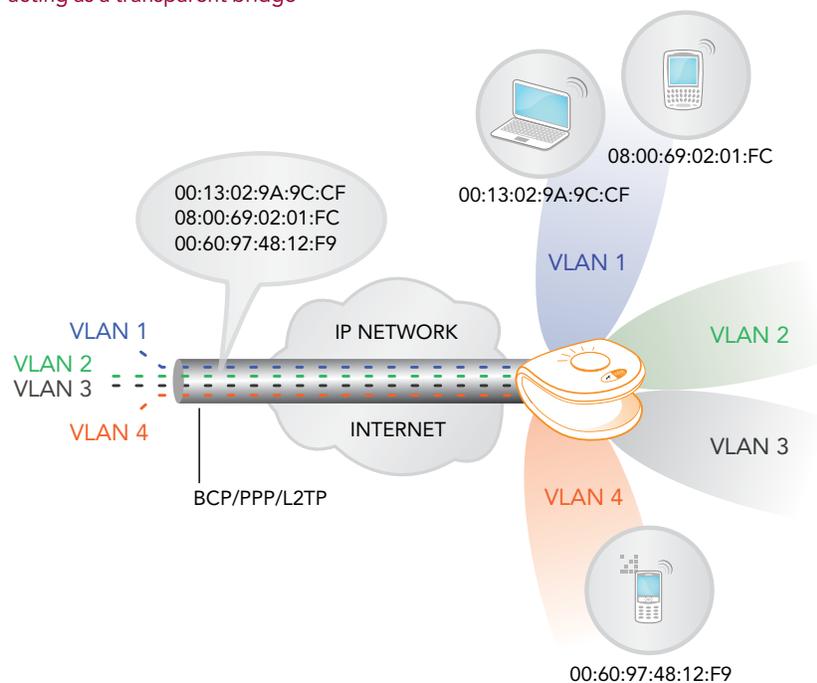
Unlike other tunnel solutions, this implementation ensures that the operator has complete visibility into MAC addresses of users, as individual Wi-Fi clients are essentially placed (bridged) onto the ISP's core network. This visibility is crucial, as MAC addresses are frequently used to grant access to the network.

Bridging using BCP also allows the operator to control IP address allocation from a central DHCP server.

The tunnelling feature augments the traffic handling features already available in the Ruckus access points. To maximize performance and enable multimedia services, QoS policies can be enforced as close to the edge as possible, even when using L2TP to tunnel traffic.

Using Ruckus SmartCast QoS technology, Ruckus APs automatically classify and prioritize voice and video traffic without any central configuration. Now hotspot operators can offer voice-over-Wi-Fi (Vo-Fi) services alongside streaming video and general purpose Internet access, delivering the best user experience possible.

VLAN tags and MAC addresses across an L2TP tunnel acting as a transparent bridge



Ruckus Wireless, Inc.

880 West Maude Avenue, Suite 101, Sunnyvale, CA 94085 USA

(650) 265-4200 Ph \ (408) 738-2065 Fx

