Clavister Feature Spotlight

Clavister L2TPv3

Creating *Virtual Wires* with L2TPv3 VPN

Top Features

- Cost-effective alternative to MPLS services
- Simplify application and server mobility
- Increase service availability
- Simplify disaster recovery and migration
- Extend the virtualized enterprise over WAN
- Increased security and privacy compared to L2 services

Introduction

There is a wide range of VPN tunneling technologies and services available on the market today. IPsec, PPTP, L2TPv2, L2TPv3, SSL, MPLS, GRE are just a few examples.

L2TPv3 sets itself apart from most other VPN protocols in the sense that it enables tunneling of Layer 2 traffic across an IP based transport network.

Up until today tunneling of Layer 2 traffic has mostly been solved through the use of relatively expensive and geographically constrained services such as L2 MPLS, dark-fibres and similar.

There are plenty of reasons why tunneling Layer 2 traffic between different locations but some very obvious and common reasons is related to the need for applications to operate as if they were located on the same LAN and during transition phases such as moving a server room from one location to another, mergers and acquisitions, mobile project offices, etc.

The use of L2TPv3 tunnels is a cost effective and flexible way to manage most of the scenarios where otherwise the expensive dark-fibres and insecure MPLS options traditionally has been used.

# L2TPv3 enhances the widely used and popular L2TPv2 Protocol

Layer 2 Tunneling Protocol Version 3 provides several enhancements to L2TPv2 for the capability to tunnel any Layer 2 payload. Specifically, L2TPv3 defines the L2TP protocol for tunneling Layer 2 payloads over an IP core network using Layer 2 virtual private networks (VPNs).

Benefits of this feature include the following:

- L2TPv3 simplifies deployment of VPNs
- L2TPv3 compliments or replaces the need for multiprotocol label switching (MPLS)
- L2TPv3 supports layer 2 tunneling over IP for any payload

L2TPv3 can also be thought of as a leased line service transported over IP and is an attractive alternative to MPLS and FrameRelay.

L2TPv3 is often referred to and described as PseudoWire or VirtualWire technology due to its nature of allowing a layer 2 network to be extended across IP based networks just as if it was done with a cable/wire.
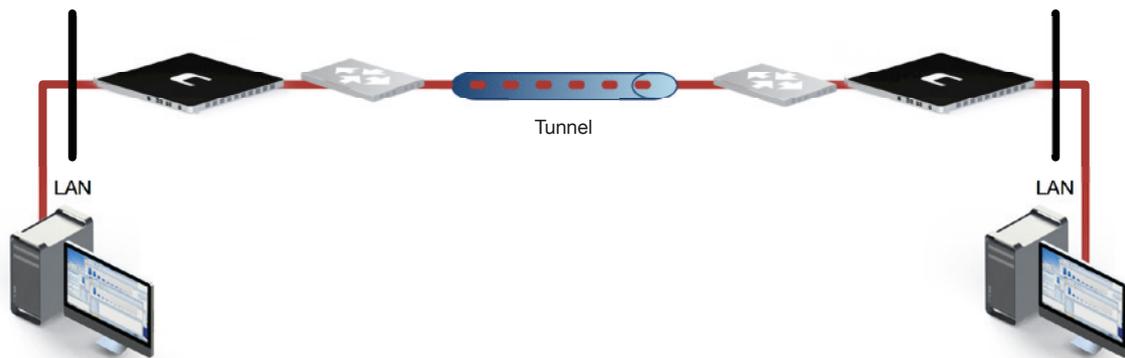
Considerations for Layer 2 Transport using L2TPv3 over WAN Links

Having the L2TPv3 protocol in place does not necessarily mean you will be able to run all applications over the link. Several restrictions apply depending on the application. For example if you intend to run VMware long distance vMotion you will need to do the math for round trip times, consider access to storage area networks and similar prior to deployment.

Platform Support

L2TPv3 Server was released in the Clavister cOS Core version 10.20 and the Client with support for IP based protocols in Clavister cOS Core 10.21.

L2TPv3 is supported on all current Eagle, Lynx and Wolf platforms available at the time of the release of Clavister cOS Core version 10.21 and that has an active maintenance service. The L2TPv3 Client with support for non-IP based protocols and an extended L2 Policy framework will be released in an upcoming version and will be available to users with an active maintenance agreement.

Scenario: Retailer Network

The use of MPLS services are very common among retail chain stores. There are several reasons why these services are popular in this type of environments but one common argument is that MPLS offer the ability to connect multiple locations together just as if they were on the same physical network.

Cost benefits

With the use of L2TPv3 the same or similar benefits can be achieved as with MPLS but at much lower cost since ADSL, 3G or 4G WAN connectivity can be utilized.

In some cases the L2TPv3 solution might replace the MPLS or L2 Services entirely and in other it might be used as a backup or load sharing alternative.

Standard ADSL, 3G or 4G services typically offer higher bandwidth capacity at a much lower cost. The need for migrating to these high-capacity, low-cost services grows exponentially as new services such as video surveillance, free guest WiFi and similar are introduced.

Security and Privacy

Thanks to all communication being end-to-end encrypted and manageable by the own organization there is significantly less risk of security and privacy issues.

When using an MPLS service there is normally no end-to-end encryption and privacy is put into the hands of the service provider. MPLS networks are typically very large and thousands of customers might be using the same routers and network equipment and there is a significant risk that a human error might result in leakage of information between different customers, possibly without any obvious signs or alarms going off.

Scenario: Remote Office Printer

For remote offices where the volume of traffic is very low the cost for connectivity can be high per printout. By adding a pair of 4G routers and using L2TPv3 the network can be configured with the network as a transparent Layer 2 tunnel. The printer will be located at the same subnet as the host but physically located far away.
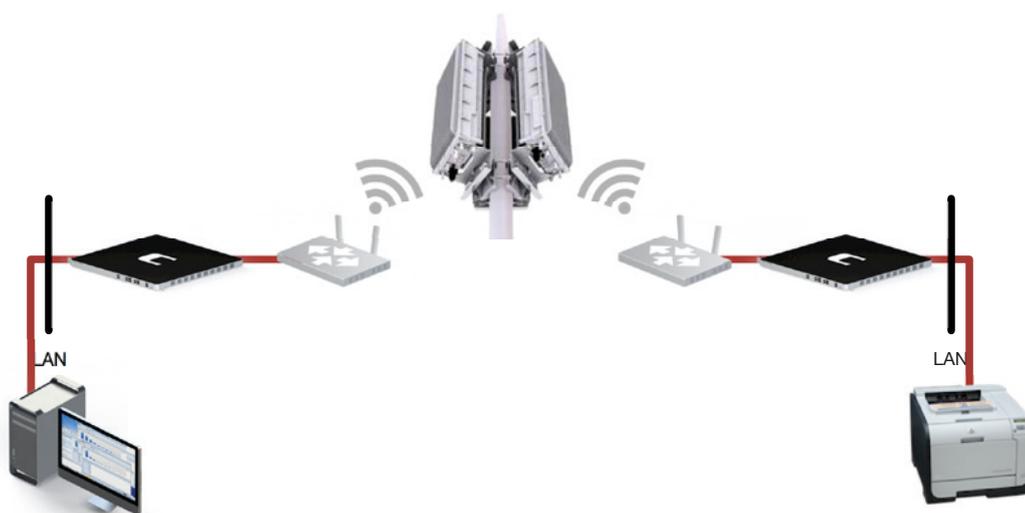
Questions and Answers

Q: L2TPv2 vs. LTPv3, what is the real difference?

A: L2TPv3 can do everything L2TPv2 can, but it is also capable of transporting Ethernet protocols such as VLANs, PPP, ATM. For this reason L2TPv3 is often referred to as "VirtualWire" technology.

Q: Can Clavister support L2TPv3 - "VirtualWires" and transport non-IP based protocols today?

A: As of the Clavister cOS Core 10.21 release, transport of non-IP based protocols over L2TPv3 tunnels is not supported. Layer 2 policies and transport of non-IP based protocols will be released in an upcoming release.

Q: Can I really replace my costly Layer 2 services with a broadband service and L2TPv3?

A: If you can replace it entirely, or if it only should be used as a backup or additional transport network, depends on many variables. The best approach is to start with L2TPv3 and a broadband service as an additional transport alternative, and evaluate the solution before deciding to decommission the layer 2 services.

Clavister L2TPv3 Key Benefits

- Cost-effective alternative to MPLS services

- Simplify application and server mobility

- Increase service availability

- Simplify disaster recovery and migration

- Extend the virtualized enterprise over WAN

- Increased security and privacy compared to L2 services

For more information about Clavister products and services, please visit us at: www.clavister.com.

Where to Buy Clavister

For more information about where to buy Clavister products, visit www.clavister.com/partners. Additional resources and customer testimonials can be found at www.clavister.com/support/resources.

About Clavister
Clavister (NASDAQ: CLAV) is a leading security provider for fixed, mobile and virtual network environments. Its award-winning solutions give enterprises, cloud service providers and telecoms operators the highest levels of protection against threats, with unmatched reliability. Clavister's performance in the security sector was recognized with the Product Quality Leadership Award from Frost & Sullivan. The company was founded in Sweden in 1997, with its solutions available globally through its network of channel partners. To learn more, visit www.clavister.com.

Where to Buy
www.clavister.com/partners

Contact
www.clavister.com/contact

CLAVISTER®

WE ARE NETWORK SECURITY

Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden
■ **Phone:** +46 (0)660 29 92 00 ■ **Fax:** +46 (0)660 122 50 ■ **Web:** www.clavister.com