

Generic Information: How YR20[®] FastL2[®] Can Be Used in Secure Edge Networks

Document Date: 2010-11-29.

Document Prepared For: Generic.

Document Prepared By: Tim Everitt, YR20[®].

Document Revision: 01.

Introduction

Telco provision of E-Line and E-LAN WAN services at OSI Layer-2 (esp. Ethernet) to customers is now well-established for three main reasons:

- The Telco has no involvement in, or access to, the customer's OSI Layer-3 (esp. IP) networks.
- OSI Layer-2 creates a much simpler service demarcation for Operations & Management.
- Many rich-media systems depend on OSI Layer-2 multicast/broadcast so corporate VLAN trunks over OSI Layer-2 WANs are becoming common.

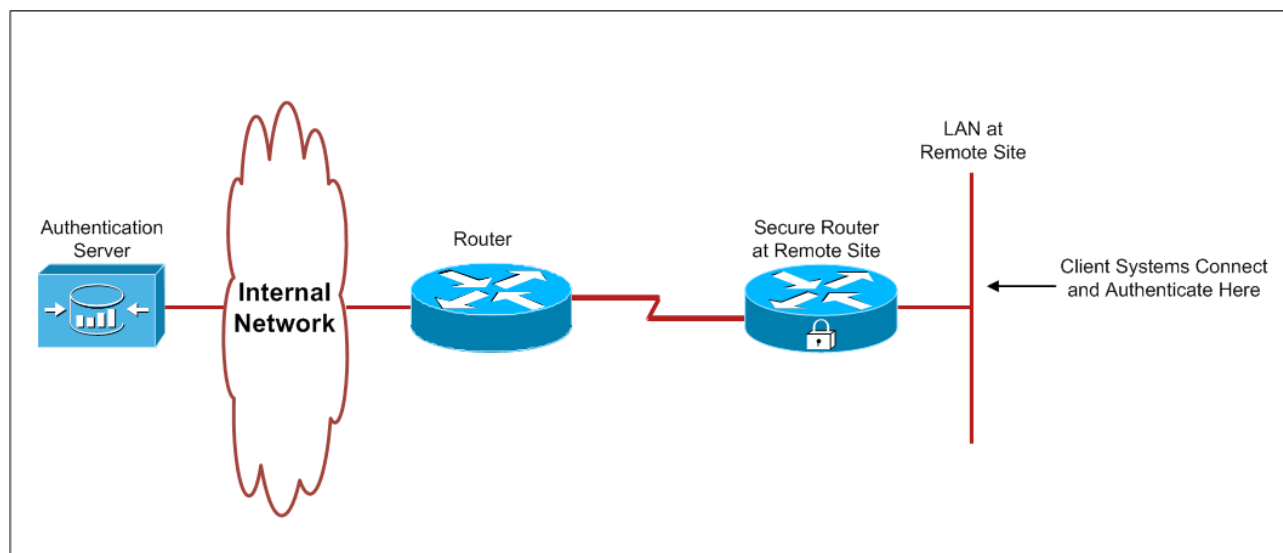
YR20[®]'s FastL2[®] patent-pending hardware, software and service creates E-Line point-to-point OSI Layer-2 (Ethernet) circuits over the public Internet. It uses the same general hub-based architecture as services such as Skype, GoToMeeting, Webex, etc to work through NAT and firewalls.

In addition to the standard OSI Layer-2 telco/customer advantages described above, YR20[®]'s FastL2[®] adds some additional benefits:

- Works from almost any Internet access service; Corp. Access, xDSL, VSAT, 3G Cellular, Inmarsat BGAN, Iridium Openport.
- Rapid Deployment; Hours (often minutes) vs. Days/Weeks.
- Additional Operations, Management & Security options.

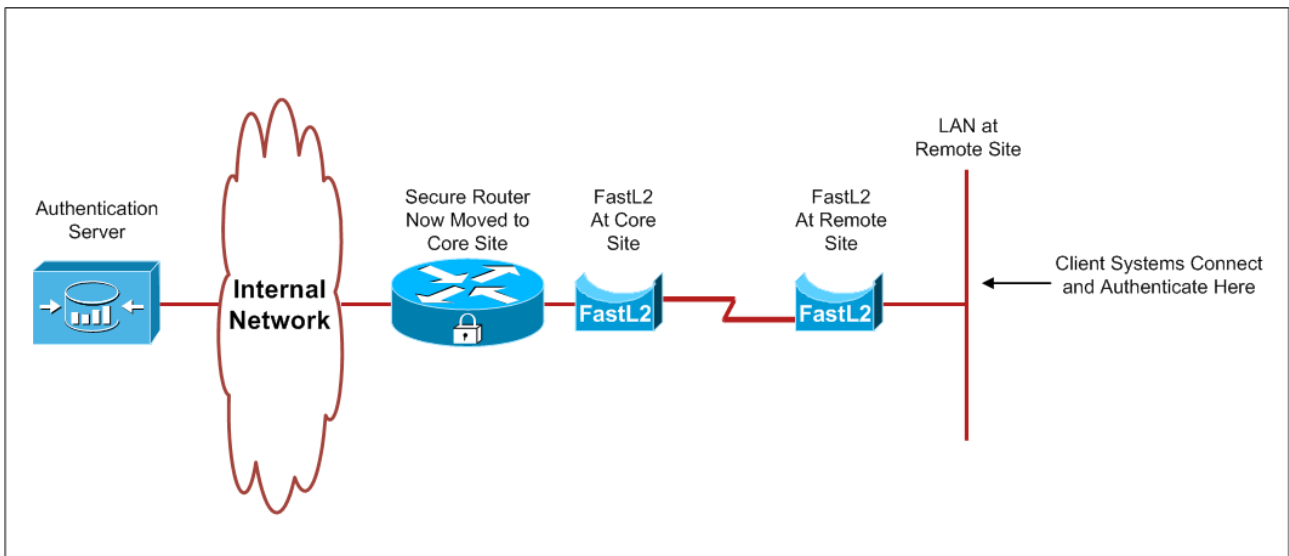
Secure Edge Networks

A common generalised architecture for secure edge networks is shown below. This is often implemented using FIPS 140-2 compliant systems and technology from companies such as Cisco, Checkpoint, Xceedium, RSA SecurID and many others.



Combining YR20®'s FastL2® into Secure Edge Networks

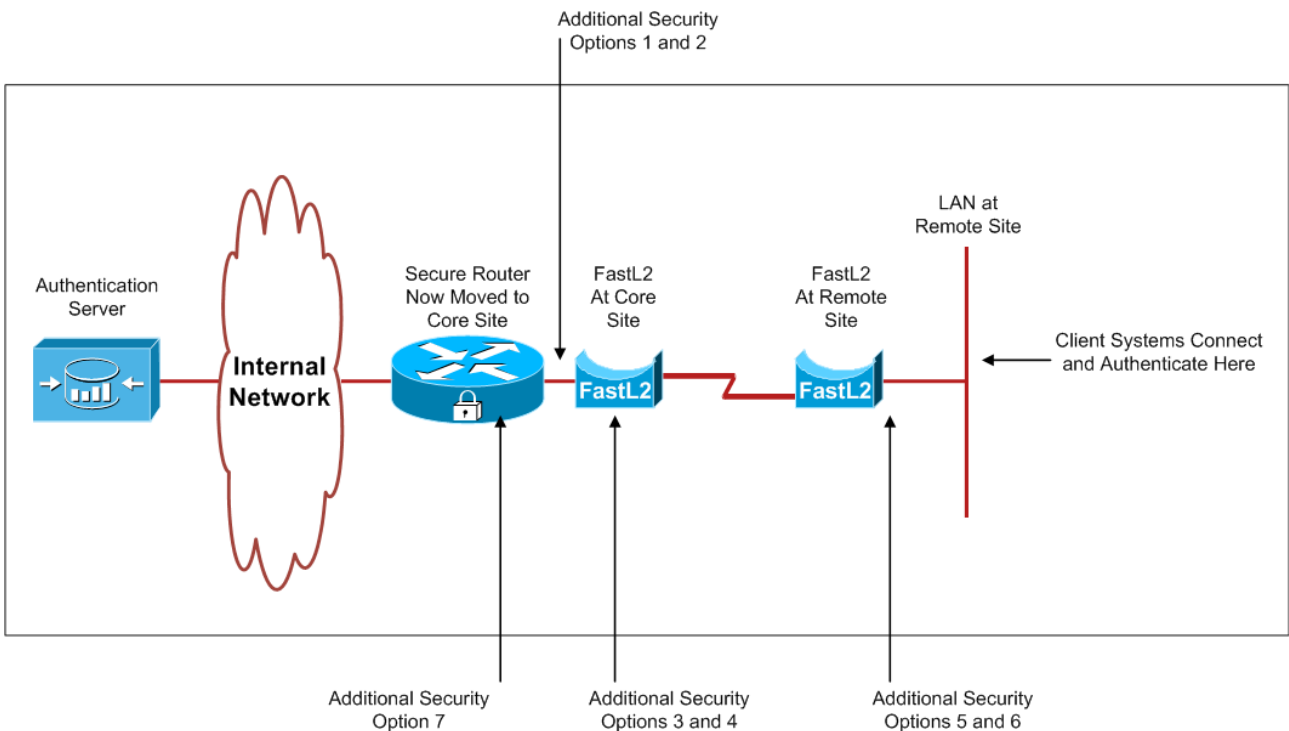
The most common architecture for combining any OSI Layer-2 carrier service into the edge of a secure network is shown below:



This architecture moves the security perimeter to the core site and uses an OSI Layer-2 Ethernet E-Line extension to a LAN on the remote site. This architecture can usually keep the existing security processes and products unchanged with the perimeter simply moved.

The YR20® FastL2® system uses well-proven standard OSS/GPL software to meet all normal requirements for WAN encryption and key management and has all the normal anti-tamper and obscuration features.

YR20®'s FastL2® introduces an additional set of Operations, Management & Security opportunities as follows:



- Option 1 is that a software or hardware traffic Test-Point can be created to allow the insertion of a customer-controlled IDS/IPS system or policy-enforcement appliance such as an Xceedium (ZeroTrust) (Note: this seems to be a preferred US Govt. architecture).
- Option 2 is that a software or hardware traffic Test-Point can be created to allow the insertion of a Test & Measurement system for Operations and QoS/SLA support. This is valuable during deployment and in-service support.
- Option 3 is that the internal FastL2[®] X-Connect that allows the traffic to flow is not enabled until completion of a customer-controlled Out-of-Band online or human/voice procedure. This can also apply to re-activation after outages.
- Option 4 is that only customer-approved Ethernet (MAC) addressed frames are permitted to pass across the network.
- Option 5 is that a USB Security Dongle must be inserted into the remote-site FastL2[®] unit before the system will activate. This can be manually over-ridden from the hub-management site on customer instruction.
- Option 6 is that the entire system, OS, FastL2[®] software, Encryption, etc. is on a secure USB Dongle.
- Option 7 is that the customer retains absolute control to automatically or manually deactivate a remote site at any time using customer-controlled systems and processes with no telco involvement.

In addition, YR20[®]'s FastL2[®] provides a rich stream of routine and event-based syslog messages which can be passed to a customer syslog server for audit and analysis.

There is a high-visibility of information at the remote site via a USB-connected LCD screen.