



ET-3300 / ET-6600 Applications

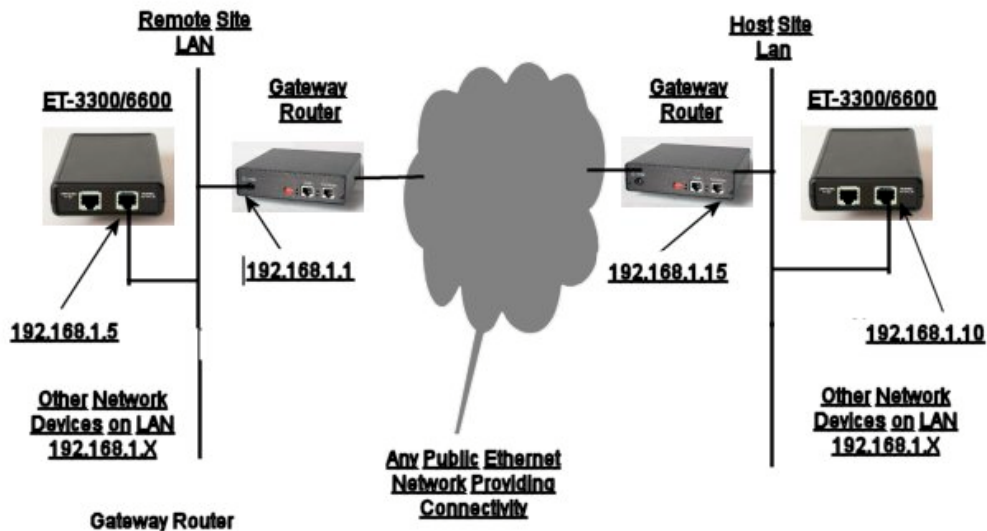
Single-Port Installation of ET Series Encrypted Tunnels

It is desirable to change the security level model a bit in some installations and run the ET tunnel in a “single-port” mode at the remote sites. The tunnel is normally installed in-line between the secured LAN and the unsecured gateway router to the other site, with the tunnel being the only device that touches both the secure and insecure LAN segments. In some smaller, less security conscious applications, this installation model doesn’t fit well with the available network topology.

The ET tunnel may be installed in these applications by using it as a single-ended bridge. That is, only one ethernet connection is used to connect the ET to the LAN. There are security implications of using this method, but the security and bridging is sufficient in many cases.

The method is simple.... Do not enable the “INSECURE” ethernet port on the ET device. If this port is left disabled, all connectivity is provided through the secure port, and the encrypted connection to the other ET device is via this same path. Include a default route or a route to the other ET device in the Ethernet-A static route table. No other changes are required in the standard installation configuration.

The ET devices at either the remote, host, or both may be used in this manner.



Example Single-Port Installation

This method does lower the security somewhat by transporting the encrypted packets on the same ethernet wire as the clear information. In strict secure installations, this is never allowed, as an attacker’s job is easier if he can compare plain text to encrypted text. In most installations, where bridging functionality is the most important feature, and the encryption is only a modest



Data Comm for Business, Inc.
2949 County Road 1000 E
Dewey, IL 61840
217-897-6600, FAX 217-897-1331
Outside Illinois: 800-4DCBNET
<http://www.dcbnet.com>

requirement, this should not provide a weakness that is easily exploitable... remember, the attack still must break the AES encryption to extract keys, and the session keys are automatically changed periodically.

The most significant security weakness this method provides is allowing the secure LAN segment to be visible to the gateway router. That opens up the ET management port to an insecure path. If this method is used, set up "Access Control" under "Administration" to limit IP addresses to those on the local network.

If the ET is used strictly for bridging without encryption as in many applications, there is no downside to using this method. The ET is used in this manner to provide a bridged link to a few nodes in a "foreign" network without having to be involved with the foreign network's configuration.

Since this method works well with ad-hock networks and small office installations, it may be used at the remote offices while the more common "in-the-path" method is used at the host site.