Application of a Virtual Private Network to the Finnish Remote Environmental Monitoring System

Heidi Anne Smartt, Susan Caskey, Robert Martinez
Sandia National Laboratories (SNL), Albuquerque, USA

Tapani Honkamaa
Radiation and Nuclear Safety Authority (STUK), Helsinki, Finland

Abstract

One of the primary concerns of employing remote monitoring technologies for IAEA safeguards applications is the high cost of data transmission. Transmitting data over the Internet has been shown often to be less expensive than other data transmission methods. However, data security using the Internet has never been adequately demonstrated. The Virtual Private Network (VPN) has emerged as a solution to this problem.

A field demonstration has been implemented to evaluate the use of Virtual Private Networks (via the Internet) as a means for data transmission. Evaluation points include security, reliability, and cost. The existing Finnish Remote Environmental Monitoring System, located at the STUK facility in Helsinki, Finland, is serving as the field demonstration system.

Sandia National Laboratories established a Virtual Private Network between STUK Headquarters in Helsinki, Finland, and IAEA Headquarters in Vienna, Austria. Data from the existing STUK Remote Monitoring System can be viewed at the IAEA via this network.

1.0 INTRODUCTION

The high cost of data transmission has become an obstacle to operating existing, or implementing new, remote monitoring systems. Sites under IAEA safeguards exist globally, and currently employ PSTN, ISDN, satellite and frame relay links for remote data transmission from the site to the IAEA. The dial-up lines (PSTN and ISDN) are typically priced by distance, which can get expensive in an international deployment. Another method for transmitting data is via courier, which can be slow, expensive, and inconvenient.

An alternative to the above is a shared public network, such as the Internet. Transmitting data over the Internet can be less expensive than other data transmission methods since the backbone is shared with many users. The major cost of implementing an Internet-based network solution becomes connecting to the Internet; this is known as the "last mile". The connection to the Internet can be accomplished via local call ISDN or PSTN, wireless, DSL, or leased line (the distance from the site to an Internet Service Provider) based on individual site geography and current infrastructure. According to Dennis Fowler in "Virtual Private Networks: Making the Right Connection":

> *Your major expenses are only the cost of that short loop that connects your office to the network access server (NAS) or POP [Point of Presence] of your Internet service provider (ISP) and your monthly Internet fee. The average price for a leased T1 (1.544 Mbps) connection is about $1,800. A typical connection from a company's offices to the local*

Sandia is a multi-program laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

DISCLAIMER

ISP's POP costs $400 to $500 a month, because the chances are you'll actually use less than a full T1 line to your POP, perhaps even a 128 Kbps ISDN line or a digital subscriber line (DSL) of some sort at an even lower cost of $50 to $150 a month. If you're a small operation, your cost may be a monthly subscription for a dial-in connection to your ISP. The savings can be considerable.

The Internet has other advantages beyond cost-effectiveness, such as scalability. With a leased line, both sites will require hardware and configuration, as well as a dedicated point-to-point connection, possibly over a long distance (Figure 1). However, by using the Internet, only the new site requires any additional hardware and configuration. Each site only has to connect to the nearest ISP thus utilizing the already-in-place infrastructure. This configuration is shown in Figure 2.

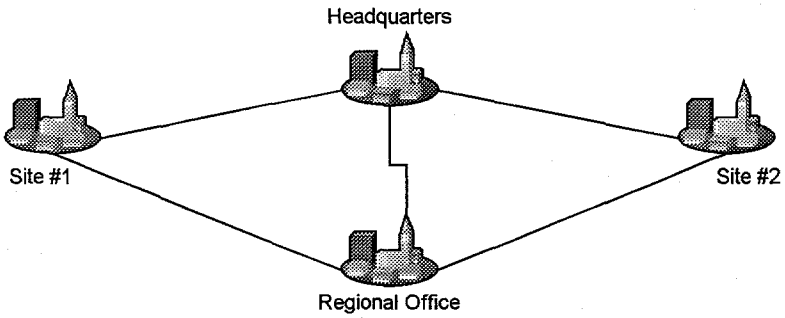


Figure 1: Leased-line Wide Area Network

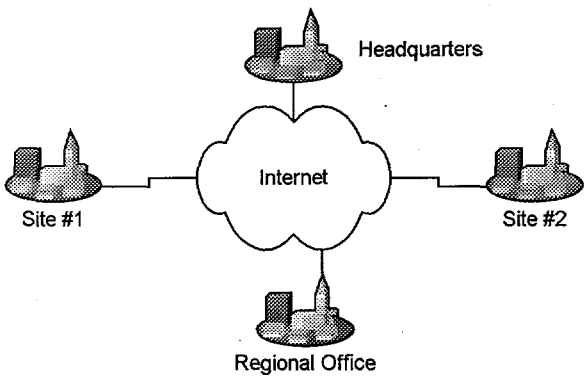


Figure 2: Internet-based Wide Area Network

Another benefit of the Internet is reliability. If a link in the Internet backbone fails during a communications session, the packets of data will automatically be re-routed and the session will not terminate. With a leased line, new routes can be defined in the event of a link failure, but the amount of time to accomplish this is too long to maintain most sessions.

The well-publicized drawback of the Internet has been the lack of data security. (However, leased lines can also be insecure since the network is also shared, albeit with fewer users.) Data can be intercepted, deleted, or modified by parties with ill intent. Virtual Private Networks (VPNs) have emerged as a solution to this problem, thus allowing the Internet to be a viable data transmission method for remote monitoring.

2.0 DESCRIPTION OF VPNS

A VPN allows secure data transmission over an untrusted public network, such as the Internet. VPN users can define encrypted and/or authenticated tunnels through the Internet. Encryption converts data from a readable format to cipher text that only the intended recipient can decipher. Most VPNs include encryption algorithms such as 3DES, DES, RC5, Blowfish, CAST, or IDEA. Authentication verifies that the data has not been altered, substituted or removed. It does this by creating a unique signature based on the data. If the data were altered, a re-authentication would show mismatched signatures. VPN data authentication can use a number of algorithms including MD5 and SHA-1. Public keys, private keys, or certificates can provide source authentication.

VPNs can be implemented in either software or hardware, and each solution has benefits and drawbacks. Software VPN solutions allows for encryption and/or authentication at each computer, rather than the hardware "gateways". Hardware has better performance, especially if using strong encryption, such as 3DES. However, the data behind the hardware will not be encrypted and thus should be in a trusted environment.

Many VPN solutions are based on the IPSec draft standard, based on TCP/IP, being developed by the Internet Engineering Task Force (IETF). The goal of IPSec is to provide a set of standards for Internet Security. Different VPN vendors are able to interoperate using IPSec.

In a non-VPN solution, a key management policy for encryption and authentication is typically manually implemented. However, with almost all IPSec-based VPNs, key management is handled by the Internet Key Exchange Protocol (IKE) and is automatic.

In an example site-to-site VPN configuration, a computer at Site A wants to send encrypted and authenticated data to a computer at Site B. The data from Site A is first fragmented into IP (Internet Protocol) packets that contain both the data and an IP header. This IP header contains the IP address of the source (computer at Site A) and destination (computer at Site B) as well as other protocol information. The IP packet is then routed through the internal network to the VPN hardware, or "gateway", which encrypts and authenticates the intercepted packet and adds a new IP header. The new IP header contains the IP address of the VPN gateways at both Site A and B, rather than the actual computers at each site. This can be an advantage, since the IP addresses of the source and destination are now hidden. The new packet is routed to the Internet, where it finds its way to the VPN gateway at Site B. The packet is now authenticated, decrypted, and sent to the appropriate destination computer at Site B. Figure 3 shows how an IP packet is handled with IPSec.

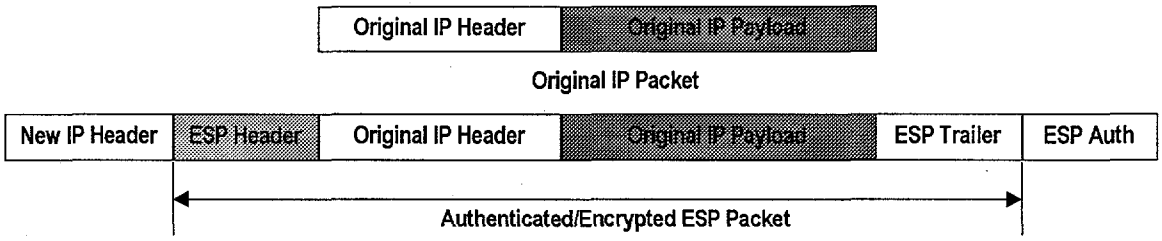


Figure 3: To convert an IP packet into an IPSec-compliant ESP packet, or Encapsulated Security Payload packet, the IP packet is encapsulated, encrypted, and authenticated.

3.0 PURPOSE OF DEMONSTRATION

The purpose of the STUK and SNL demonstration is to evaluate VPNs using the following criteria: cost-effectiveness, reliability, and security on behalf of the IAEA. The evaluation began after the installation in May 2000, and will end in October 2000. STUK, the IAEA, Nokia, and Sandia National Laboratories will all participate in the evaluation.

4.0 VPN ARCHITECTURE BETWEEN STUK AND IAEA

The demonstration linked an existing remote monitoring system at STUK headquarters in Helsinki, Finland, to the IAEA in Vienna, Austria. STUK had previous Internet connectivity and thus the installation and configuration of VPN hardware was relatively simple. The VPN hardware was installed behind the STUK firewall, and the firewall was configured to allow key management and encrypted traffic into the network. Through the VPN management software, the VPN hardware was configured to allow any VPN client, with the appropriate authentication certificate, access to the data.

At the IAEA, VPN client software, the encryption keys, the appropriate certificate, the security policy (which includes the agreed-upon algorithms for encryption and authentication, and re-keying intervals) and CompuServe software were installed on a computer. Once a connection to the Internet was established, the VPN client software began a secure negotiation with the VPN gateways in Finland, and a secure tunnel was established to view the data. Appendix A shows the system diagram.

5.0 INITIAL EVALUATION RESULTS

Since installation, the VPN hardware has been operating continuously. The IAEA VPN software client established reliable connections to the hardware during the demonstration. Currently, SNL uses another VPN software client to test the reliability each day. The reliability of the connection between SNL and STUK has been 100%.

No security problems have been discovered to date. The VPN hardware and software have been configured for 3DES encryption, HMAC SHA-1 data authentication, and certificates for source authentication. Encryption re-keying occurs every hour, and data authentication re-keying occurs every 8 hours. Encryption can be verified using a network sniffer.

In a VPN solution, every access point on each end must be secure. It is possible for an attacker to install a program on one of the end point systems, which would allow them to use the VPN to access the system on the other end without detection. Therefore, it is imperative to not allow any access to the Internet other than across the VPN. In the current demonstration system, the Material Monitoring System (MMS) computer at STUK is connected only to the VPNs, and the IAEA can use a "stand-alone" computer to dial-out to CompuServe. Thus both end point systems are secure.

Several cost-benefit analyses are shown in Appendix B. It is important to note that each cost-benefit analysis will vary based on the current method for transmitting data, facility type and geographical location. The analyses provided are for specific scenarios only. The first shows the cost-benefit of the VPN link between STUK and the IAEA. Due to the high data connection rates for modems at the STUK and IAEA sites, the small amount of data (unrealistic for a remote monitoring site), and the labor costs of implementing VPNs, a VPN solution would not be cost-

effective for this system (assuming the only host at STUK is the MMS computer). An increase in the amount of data, or the number of VPN applications (such as remote access for e-mail or protecting other computers or networks), would significantly change the cost-benefit. For example, increasing the amount of data to 25 Mbytes per day and keeping all other factors constant, the payback period would be 16 months (this is shown in a second column). Comparing the monthly operating costs for 25 kbytes of data per day to 25 Mbytes shows that the modem cost is directly proportional to data amount. With the Internet, cost is independent of data amount. The following is another example of cost-benefit using a different data transmission method: A 64 kbps private leased line between Helsinki and Vienna was quoted at $2153 for start-up costs, and $2258 per month. Comparing this to the VPN solution (and not including the start-up costs), the payback period for VPNs would be approximately 11 months, and the return on investment 2%.

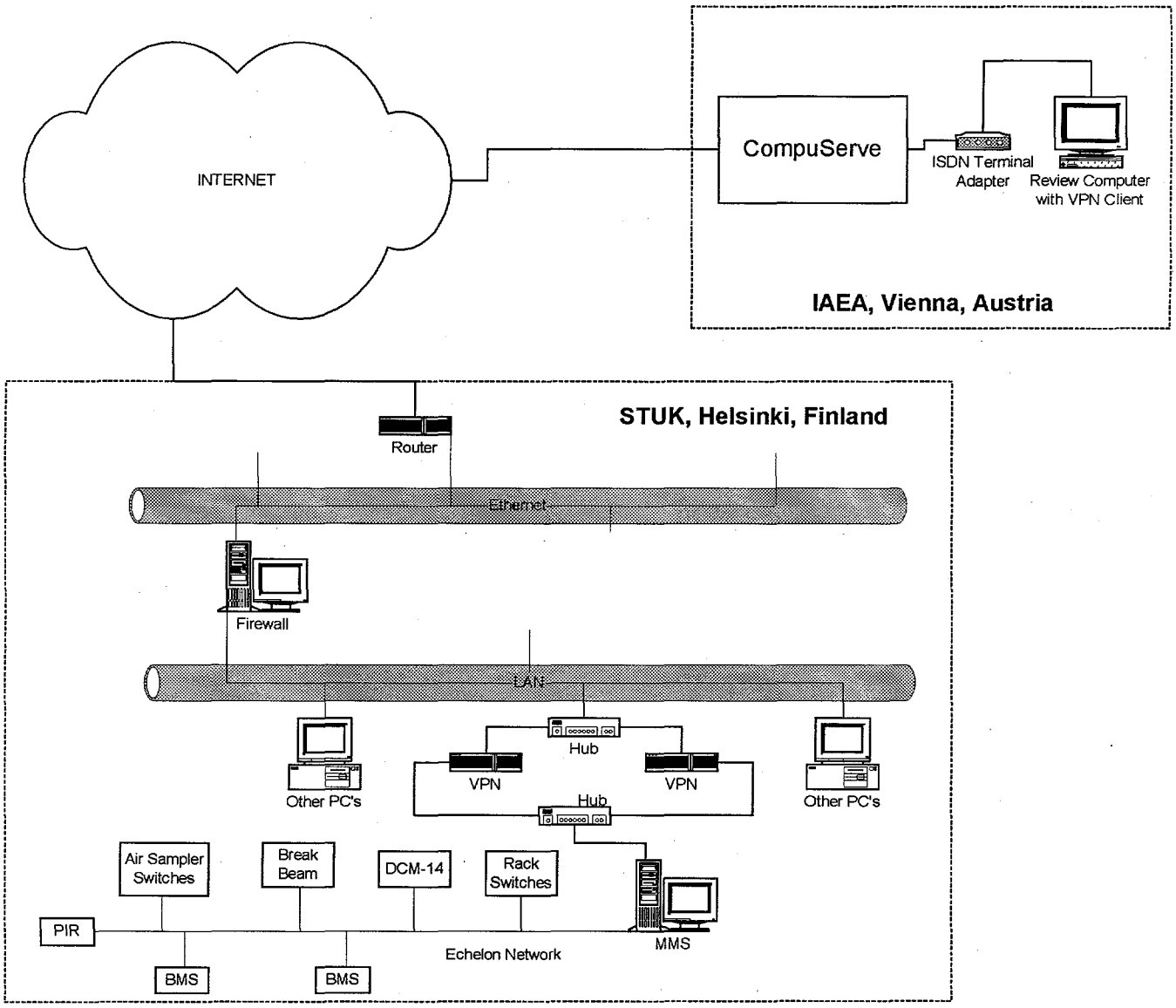
The second analysis shows an IAEA/Embalse-type site-to-site implementation. It is assumed that VPNs would be added for the first time at both sites. Here, the cost-effectiveness is significant because of low data transmission rates, large amounts of data, and a higher long-distance phone rate. Notice that the analysis assumes that the remote site does not have any access to the Internet. Many alternatives exist for connecting to the Internet, but a full T-1 line has been chosen for this analysis. The cost of a T-1 line installation and operation were not available for Argentina, and therefore, U.S. rates are shown. However, since U.S. rates for communications are typically much lower than other countries, the rates were doubled in the model. Other assumptions in this example are that both the IAEA and the Embalse-type site networks can support a VPN solution. Factors that might be an obstacle include topologies other than Ethernet, Network Address Translation, and firewalls that do not allow protocols required for VPNs. Also, it is assumed that support and maintenance for a VPN solution would be about the same as that for the current method of data transmission. Furthermore, it is assumed that the IAEA would be implementing a full VPN solution for remote monitoring, thereby necessitating the use of a larger-throughput (and more expensive) VPN.

The third analysis shows a "second" Embalse-type implementation. In the second implementation, the IAEA will already have VPN hardware. Labor costs for the IAEA would include defining (in software) a tunnel between the two sites. This requires on average less than an hour of labor, and therefore is not included in the analysis. The new site will require additional hardware and implementation costs, such as network planning. The cost-effectiveness of this scenario is greater than that of the first site/IAEA implementation.

6.0 CONCLUSION

A properly configured VPN solution provides a secure method for data transmission across the Internet. The Internet can allow cost-effective, scalable, and reliable communication methods between two or more sites. However, it should be emphasized that a cost-benefit analysis must be performed for each site or application. The combination of ensured data security and potential low operating costs make VPNs an attractive alternative for both intra-site and inter-site data transmission. That, in turn, makes remote monitoring a much more effective and efficient tool for accomplishing the IAEA mission of International Safeguards.

APPENDIX A: STUK/IAEA Virtual Private Network Diagram.



APPENDIX B: Cost-Benefit Analyses.

STUK/IAEA - MODEM VS. CLIENT-TO-SITE VPN				
DATA TRANSMISSION VIA TELEPHONE	**(LOW DATA AMOUNT)**		**(HIGH DATA AMOUNT)**	
Bytes/Day of Data	**250,000**		**25,000,000**	
Lowest Modem Connection Data Rate (bps)	33,000		33,000	
Time to Download/Day (in minutes)	1.01		101.01	
Cost/Minute	$0.52		$0.52	
Total Operator Charges $0.08 per 7 minutes	$0.01		$1.15	
Cost Per Day to Download Data	$0.54		$53.68	
MONTHLY OPERATING COSTS (30 DAYS)	**$16.10**		**$1,610.39**	
DATA TRANSMISSION VIA VPN				
CAPITAL EQUIPMENT	**Quantity**	**Cost**	**Total**	
Nokia VPN Hardware (Model 500)	2	$1,995.00	$3,990	
Ethernet Hubs	2	$171.75	$343.50	
Ethernet Card for PC	1	$200.00	$200.00	
Miscellaneous Cables	10	$3.95	$39.50	
VPN Client Software License	1	Inc. w/ HW	$0.00	
CompuServe Software	1	Free	$0.00	
ISDN Terminal Adapter	1	IAEA	$0.00	
TOTAL EQUIPMENT COST			**$4,573.00**	
IMPLEMENTATION COSTS (LABOR)	**Days**	**Persons**	**Cost/Day**	**Total**
Network Information Gathering	1.5	1	$1,000.00	$1,500.00
VPN Installation Planning	2	2	$1,000.00	$4,000.00
Simulate in Lab (Sandia)	2	2	$1,000.00	$4,000.00
VPN Installation (Hardware - at STUK)	1.5	1	$1,000.00	$1,500.00
VPN Installation (Client/CompuServe at IAEA)	1	1	$1,000.00	$1,000.00
Training (Two Sandia employees)	5	2	$1,000.00	$10,000.00
TOTAL LABOR				**$22,000.00**
TOTAL CAPITAL COSTS (LABOR + EQUIPMENT)				**$26,573.00**
MONTHLY OPERATING COSTS (INTERNET ACCESS)				
STUK*	$0.00			
IAEA (CompuServe Account)**	$0.00			
TOTAL OPERATING COST PER MONTH	**$0.00**			
PAYBACK PERIOD (IN MONTHS)	**1,650.10**	(LOW DATA	**16.50**	(HIGH DATA
RETURN ON INVESTMENT	**-99.27%**	AMOUNT)	**-27.26%**	AMOUNT)

*STUK already has Internet access and doesn't anticipate additional costs from VPNs.

**IAEA has a CompuServe account for the Safeguards Department and doesn't anticipate additional costs from VPNs.

EMBALSE-TYPE SITE/IAEA - MODEM VS. SITE-TO-SITE VPN	
DATA TRANSMISSION VIA TELEPHONE	
Bytes/Day of Data	25,000,000
Lowest Modem Connection Data Rate (bps)	9600
Time to Download/Day (in minutes)	347.22
Cost/Minute (assumed)	$1.00
Cost Per Day to Download Data	$347.22
MONTHLY OPERATING COSTS (30 DAYS)	**$10,416.67**

DATA TRANSMISSION VIA VPN SITE-TO-SITE				
CAPITAL EQUIPMENT	**Quantity**	**Cost**	**Total**	
Nokia VPN Hardware (Model 500)	2	$1,995.00	$3,990	
Nokia VPN Hardware (Model 2500)	2	$9,995.00	$19,990	
Ethernet Hubs	4	$171.75	$687.00	
Ethernet Card for PC	2	$200.00	$400.00	
Miscellaneous Cables	12	$3.95	$47.40	
Start-up Costs for Internet Access, if required	1	$6,000.00	$6,000.00	
TOTAL EQUIPMENT COST			**$31,114.40**	
IMPLEMENTATION COSTS (LABOR)	**Days**	**Persons**	**Cost/Day**	**Total**
Network Information Gathering	2	2	$1,000.00	$4,000.00
VPN Installation Planning	5	2	$1,000.00	$10,000.00
Network Preparation	1	2	$1,000.00	$2,000.00
VPN Installation	2	2	$1,000.00	$4,000.00
Training	3	2	$1,000.00	$6,000.00
TOTAL LABOR				**$26,000.00**
TOTAL CAPITAL COSTS (LABOR + EQUIPMENT)				**$57,114.40**
MONTHLY OPERATING COSTS (INTERNET ACCESS)				
Remote Site (Assuming no Access)*	$5,190.00	*Provided by UUNet 8/97		
IAEA	$0.00			
TOTAL OPERATING COST PER MONTH	**$5,190.00**			
PAYBACK PERIOD (IN MONTHS)	**10.93**			
RETURN ON INVESTMENT	**9.81%**			
SECOND EMBALSE-TYPE SITE/IAEA - MODEM VS. SITE-TO-SITE VPN				
CAPITAL EQUIPMENT	**Quantity**	**Cost**	**Total**	
Nokia VPN Hardware (Model 500)	2	$1,995.00	$3,990	
Ethernet Hubs	2	$171.75	$343.50	
Ethernet Card for PC	1	$200.00	$200.00	
Miscellaneous Cables	7	$3.95	$27.65	
Start-up Costs for Internet Access, if required	1	$6,000.00	$6,000.00	
TOTAL EQUIPMENT COST			**$10,561.15**	
IMPLEMENTATION COSTS (LABOR)	**Days**	**Persons**	**Cost/Day**	**Total**
Network Information Gathering	1	1	$1,000.00	$1,000.00
VPN Installation Planning	2.5	2	$1,000.00	$5,000.00
Network Preparation	1	1	$1,000.00	$1,000.00
VPN Installation	2	1	$1,000.00	$2,000.00
Training	3	1	$1,000.00	$3,000.00
TOTAL LABOR				**$12,000.00**
TOTAL CAPITAL COSTS (LABOR + EQUIPMENT)				**$22,561.15**
MONTHLY OPERATING COSTS (INTERNET ACCESS)				
Remote Site (Assuming no Access)*	$5,190.00	*Provided by UUNet 8/97		
TOTAL OPERATING COST PER MONTH	**$5,190.00**			
PAYBACK PERIOD (IN MONTHS)	**4.32**			
RETURN ON INVESTMENT	**178.00%**			