GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Confidentiality of Information on Dedicated Leased Lines

William M. Karwisch Jr.
May 1, 2003
GSEC Practical Assignment
Version 1.4b

Abstract

Security decisions are based on a number of foundational assumptions. The effectiveness of any decision depends on the soundness of the underlying assumptions. To ensure that security is adequate and will work, these assumptions need to be examined. Any time we hear that "A" is secure (or insecure) because of "B", we need to ask some questions. Why that is true? How do we know? What do we know about "B" that makes "A" secure or not? This questioning must be done without bias and without assuming that the conclusion is known in advance.

One assumption frequently heard is that a wide area network (WAN) is secure because its sites are linked using dedicated leased lines. Many people believe that these lines are inherently secure. Some providers of these lines certainly advertise them as secure.

It is unsound to assume without question that dedicated leased lines are secure. This paper examines the properties of leased lines and the reality about their security. The main focus is the risk of loss of secrecy of information transmitted on dedicated leased lines. (The discussion of other aspects of security of dedicated leased lines, such as the analysis and risk-mitigation related to loss of service, will be left to others.) This paper reviews the evolution of dedicated leased lines and discusses how this influences their security. It examines the decisions made by telephone companies in response to competitive pressures and how these decisions may impact security.

The examples here are commonly used point-to-point services with DS1 and DS3 lines (T1 and T3). Not discussed is the security of the end-points, which is essentially the same irrespective of the line type. A full discussion of all types of dedicated leased lines (which include optical, microwave, satellite, radio and other transmission media) is beyond the scope of this paper; although many of the concepts discussed here apply to them. The discussion of dedicated leased lines that connect with ISPs and frame-relay services will also be limited, but many of the concepts apply to them as well.

The Myth of Inherent Security

Frequently there is a need to transmit information securely from one location to another. More specifically, there is a requirement that information be communicated dependably when needed, while protecting it from disclosure to unauthorized parties. The key attributes of the communications link are availability, reliability and confidentiality.

A popular choice for meeting these requirements is a point-to-point dedicated leased line. The reliability and availability of leased lines is as good as the industry has to offer.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

It is available because it is always connected and the bandwidth of the circuit is dedicated. It is reliable because the circuit uses fixed routing (although this is not always strictly true, as will be discussed later) and the service can be managed from end-to-end.

Dedicated leased lines are sometimes used with the assumption that the communications they carry will remain confidential. The reasoning is that they must be secure because attackers cannot connect to them over the Internet, vendors market them as secure, and many people refer to them as private lines. The lack of ubiquitous access to private lines from the Internet provides significant security; however, one should never accept marketing claims without checking the facts. Private, in this case, means only that the telephone company reserves the line for the customer's exclusive use. Some telephone companies, such as BellSouth ("BellSouth® Long Distance"), clearly market private lines as providing guaranteed capacity with managed service, without making claims about security.

Other vendors market private lines, without qualification, as secure. MCI ("Metro Private Line") is one example: "MCI, an inter-exchange carrier, now offers local service over its own local network facilities. MPL has the bandwidth capacity to provide your company with a flexible, secure, and cost-effective intraLATA (Local Area Transport Area) private line solution." Telenor Business Solutions ("Internet Services") is explicit: "How secure is the Leased Line service? A Leased Line is inherently secure in it's own right because it operates as a point-to-point service."

Once the decision is made to use a leased line, it is frequently assumed that there is no need to take additional measures to preserve confidentiality of data transmissions. Although confidentiality is easily accomplished on leased lines, the vendor does not typically guarantee it. In fact, AT&T ("AT&T Business"), MCI ("General Terms") and Sprint ("Schedule No. 7"), among others, specifically absolve themselves, by the terms and conditions of their service agreements, of any liability resulting from loss of confidentiality or unauthorized access.

The overall security of a system results from the security (or lack of security) of each of its components. The security of a network that uses a dedicated leased line depends on the security of the line. To evaluate the security of the line, one must look beyond marketing claims. Too often, the security of a line is uncritically accepted without examining the security of its components. This failure helps to perpetuate the myth that they are inherently secure. Although leased lines are not frequently compromised, compromises that do occur are seldom publicized, which does little to dispel the myth.

The Reality of Leased Lines

Leased lines have limitations and vulnerabilities that should be considered and mitigated when using them as components of networks. These lines are vulnerable to two main categories of incidents: denial of service and loss of secrecy.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Denial of service may be a result of accident or attack. Construction work occasionally damages these lines. An attacker may intentionally cut them. If an update to a master database of an inventory system were delayed by loss of service, there may be little or no damage. But if an emergency response system did not work, the result could be catastrophic. Regardless of the impact, an outage would be obvious. The risk of loss of service is either accepted or mitigated by providing redundant circuits and routes.

Denial of service is an obvious problem, but loss of secrecy of information is a subtle problem. Like denial of service, the damage done by loss of secrecy depends on the application. Unlike the loss of service, however, compromised secrecy may not be detected at all. If someone captures your information without getting caught, without disrupting your service, and without telling you, how would you know it happened? Even if detected, the appropriate action may not be obvious. Sometimes, nothing would be sufficient to mitigate the damages. Once a secret is revealed, it cannot be made secret again.

Dedicated leased lines provide a degree of security because ubiquitous access is not available. Random attacks are not likely to occur. Virtually all attacks on these lines are specifically targeted. Physical access is risky; wiretapping and eavesdropping are difficult and illegal. While this will keep out casual attackers, one should still be concerned about the possibility of a skilled and motivated attacker who may target a specific leased line for a specific reason.

Linder (2001) correctly points out that “private leased-line facilities are vulnerable to some of the same security threats as the IP-based bearer networks. However, the lack of ubiquitous access to private line implementations makes protection of these networks easier to implement and sustain.” His paper continues to discuss “securing networks from the Internet and other un-trusted IP-based bearer networks.” This implies that private leased lines may be part of a trusted network. How far this trust extends will be discussed later in this paper.

The risks are not new – information has been available for many years. It was publicly discussed in depth on the Internet as early as 1995. (This information was not new then; leased lines are much older than the Internet. The point is that the Internet made this information widely and publicly available years ago.) Maillet (1995) triggered an interesting discussion thread when he wrote, “If we use didicated [sic] leased lines from the US to Europe (say from AT&T or MCI), can someone in between get our data? What about if [we] used a “cloud” style network like ATM or Frame Relay which use PVCs instead of a dedicated curcuits [sic]?” Responses show that several individuals were very aware of the implications and include discussions of the risk, modes of attack and anecdotal evidence of interceptions that had already occurred.

For applications that have a critical dependency on maintaining the confidentiality of information, trusting leased lines may not be appropriate. Assuming that a calculable loss could result from a compromise, the value of the risk is calculated to be the cost of the loss multiplied by the probability that a compromise will occur. In the case of loss of

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

secrecy, however, the estimates for both the loss and the probability of occurrence are difficult to quantify. Attempts to fix the value of the risk tend to be imprecise because the loss value can be extremely large, while the probability of occurrence value can be extremely small. Still, if the cost of mitigating the risk were judged to be low in comparison to the potential for damage, mitigation would be prudent. In any case, if the cost of mitigation is less that the value assigned to the risk, mitigating the risk is the correct approach.

The discussion of quantifying the cost associated with compromised confidentiality is outside the scope of this paper. It is obvious, however, that the cost would be unacceptable in many cases. One case would be where national security was compromised. Another case would be where a company's competitive advantage was lost because its proprietary information had been made public. Another case would be where a financial institution inadvertently disclosed sensitive customer data and transactions to unauthorized individuals.

The difficulty in quantifying the probability that a compromise will occur results from the difficulty of quantifying the underlying components of risk, including:

- Assessing risk of exploiting underlying technologies
- Assessing risk attributable to extended trust relationships
- Assessing the motivation for targeting a particular leased line
- Obtaining reliable historical statistics for actual compromises
- Establishing the number of actual compromises that go undetected

One should compare the cost of mitigating the risk with the value calculated for the risk to determine whether mitigation is the correct approach, but evaluating the risk may be prohibitively difficult and expensive. One may decide that the potential for loss is great enough and the cost of mitigating the risk is low enough to justify mitigation without a formal evaluation.

The need for VPNs on public switched networks (PSNs) is clear and is evidenced by the wealth of research and articles on the subject and the number of VPN products available. They provide confidentiality, prevent easy unauthorized access at end points, and prevent man-in-middle attacks. Data that is intercepted in transit is useless to an attacker. These traits are just as desirable for private, leased facilities as they are for public networks. Proper risk evaluation must be performed in both cases. The conclusion that mitigation of risk is not necessary for either public or private networks should be the result of careful analysis.

Point-to-Point Communications and the Telecommunications Network

The need to provide cost effective service has driven the development of telecommunications technology. Pressure to be cost effective has been sometimes the result of regulatory action and sometimes the result of competition, but has remained a

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

constant throughout the development of the industry. To fully understand today's telecommunications technology and how it applies to point-to-point, dedicated leased lines, it is useful to understand how it evolved.

By the time the need for wide-area data communications emerged, the telephone network had already matured. Adapting the existing technology to meet these emerging needs was natural and cost effective. Existing technologies were adapted to meet the emerging needs of data communications. Telecommunications companies used (and still use) multiplexing, sharing of facilities, and other techniques to maximize utilization of their resources and deliver service at the lowest possible cost.

Probably the simplest example of point-to-point communication is two people talking directly with each other (without a telephone). Of course, eavesdropping is always a possibility; so, if secrecy is required, they can find a private location for their conversation. As the distance between them increases, the difficulty of having a private, real-time conversation increases. The telephone was invented to solve the problem.

Alexander Graham Bell's famous first telephone used a true, dedicated, point-to-point, and private telecommunications line. (Although not leased, it was indeed owned by what was to become the “telephone company.”) The two sets were connected to the endpoints of the line, which had no other connections and was dedicated for their exclusive use.

As the number of people who used telephones increased, it became obvious that a separate point-to-point connection between each distinct pair of people that wanted to talk would not be feasible. The central office was born. All telephone lines went from the home or business to the central office. At first, the lines were directly connected to switchboards. When someone wanted to make a call, an operator physically connected the line from the calling party to the line connecting the called party using a patch cord, thus establishing a circuit between the two phones.

An important privacy problem emerged – the operator had a headset and could eavesdrop on the conversation. The eavesdropping operator became a cliché, which is frequently parodied, as in Lily Tomlin’s portrayal of the operator, “Ernestine.”

Later, phones had rotary dials and the primary duty of connecting calls was assigned to electro-mechanical switches that counted the pulses from the rotary dials. Eventually, the pulse-counting systems gave way to tone systems that use computer switching – the systems that we use today.

All the lines were collected and switched at the telephone company's central office. (The central office, with its switches, is analogous to the Ethernet switches and routers that we use to connect our computer networks.) If a call could be connected locally, the switch did so. Of course, each central office needed to handle calls for lines to which it was not connected. Lines were installed between central offices for this. If the call could not be connected locally, the switch made a routing decision and the circuit was

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

connected to a switch at another location, which had the responsibility of completing the call.

The number of calls that could be simultaneously connected between any two offices depended on the number of lines that were available. When a line became free, it was available for another call. Sharing capacity in this way maximized the efficiency of calls, but it created the situation that when all the lines were busy, a call could not be connected. To meet increasing demands, the companies installed more lines. Just a few decades ago, it was not unusual to see cross-country installations that contained dozens of individual wires spaced evenly in large arrays from pole to pole.

In 1927, Harry Nyquist of Bell Labs determined how to convert analog signals to digital. Nyquist determined that 64,000 bps were required to adequately convert a voice conversation to digital. This work led to the development of the DS0 signal, which is “the basic building block of modern communications.” (“How do we convert”)

In 1962, Bell Labs developed the T1 carrier, which could multiplex 24 DS0 signals together into the DS1 signal that the T1 carrier transmitted. The standard DS1 lines that we still use today are the implementation of T1 on twisted-pair copper wires. Similarly, 28 DS1 signals can be multiplexed together into a DS3 signal, usually referred to as T3.

The conversion of analog to digital and the multiplexing of circuits allowed increased call density on the telecommunications companies’ facilities. Bell Labs (“T1 Carrier”) says, “One of the interesting features of T1 was that the 1.544 Mb/s signal was being transmitted on the same 24-gauge twisted-pair copper wire that was used as subscriber lines to connect customers' telephones to the central office switch. The use of this 24-gauge wire made it possible for telephone companies to greatly expand their networks in urban areas, where many cable lines were run in underground conduit that had reached their capacity.”

DS1 and DS3 lines require repeaters at regular intervals to prevent loss of signal due to attenuation on copper lines. The economics of transmitting over long distances favored microwave and satellite as the transmission media. Eventually, fiber-optic cable replaced copper and microwave as the medium of choice for transmission over long distances because it allows even higher transmission density and can transmit over great distances very economically. However, T1 and T3 remain popular choices for end-point service connections, such as an end-user’s PBX or WAN connection.

Remote Data Communications using Leased Lines

The development of the telecommunications network predated the development of computers. When computers were ready to communicate with each other, telephone companies found themselves in the enviable position of being able to use their existing infrastructure to provide data communication services to their customers. The technology that was developed to multiplex many voice calls together on a single line was ideal for transmitting large amounts of data over long distances.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Automated data communications occurred much earlier than the first computers. According to Nelson (1963), Frank Pearne had begun work on the first Teletype machine as early as 1902. The Teletype business developed steadily over the next several decades before computers arrived on the scene.

In the 1950's, communication between computers was slow and customized. Modems were developed to communicate using the Public Switched Telephone Network (PSTN). There was no consistent, universal approach to interconnect computers. The ARPANET project in 1969, which eventually resulted in the Internet, allowed computers to connect according to defined standards. Digital signaling was already in place at the telephone company and was ideal for internetworking computers.

Today, because of the wide availability of telecommunications infrastructure, one rarely has the need to install and operate one's own WAN infrastructure. Telephone companies provide dedicated leased lines to connect WANs. "Leased" means that the line is owned by the telecommunications company and is used by the customer for a fee. This is a contractual arrangement for the use of the line and has no bearing on security. "Dedicated" means that the line is reserved for the exclusive use of the customer. Two questions need answers: what is dedicated and for what period of time?

A line is dedicated when it is reserved for a specific use. In a limited sense, the circuit used for an ordinary voice call is dedicated. Once the circuit is established, the connection and the bandwidth is allocated and reserved for the exclusive use of the caller for the duration of the call. To request such a connection, a caller needs only to pick up a handset and dial a number. Of course, there is no guarantee that the facilities will be available at the time the call is placed – the caller could get a busy signal.

To request a dedicated leased line, one must call the telephone company's sales representative and place an order. Again, there is no guarantee that the facilities will be available at the time the request is made. However, once connected, contracts for dedicated lines specify that the line will be reserved for the exclusive use of the customer for the duration of the contract. So one important distinction between dedicated and non-dedicated lines is the length of time during which the line is reserved. However, the duration of the connection has little relevance with respect to security. In fact, one might argue that everything else being equal, a longer-term connection may be more vulnerable than a shorter-term connection because an attacker would have more opportunity to research and revisit the target.

Some specialized installations use facilities installed by the telephone company that are routed directly from one location to another. These are rare because they generally cannot use the telephone company's existing facilities – new wiring must be installed for the entire length of the circuit. Also, such circuits cannot be monitored or managed by the vendor because of the lack of connections to the wiring.

Most point-to-point, dedicated leased lines use local loops that connect the end points to the vendor's central office where the connection is made. If the end points connect to

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

different central offices, arrangements are made by the vendor to complete the circuit between the central offices.

Provisioning, in telephone company terminology, is the process of connecting the end points of a line through the various pieces of interposed equipment that complete the circuit. It is possible to provision a point-to-point line using direct connections. Even when the line passes through a central office, the line can be manually connected, bypassing other equipment.

Manually connected lines reduce the risk of being compromised because they are connected to fewer pieces of interposed equipment. However the goal of security in this case competes with the goal of offering cost-effective, manageable service. A manually connected line cannot be easily monitored or managed. In addition, manual connections are labor-intensive and expensive.

To make the lines manageable and cost effective, telephone companies usually provision local loops using specialized switches called digital cross-connect switches (DCSs). According to Sunrise Telecom ("Working with T3"), "DCSs commonly reduce the space required for achieving channel cross-connection, eliminate the manual labor associated with cross connection, and can provide amazingly fast computerized rerouting of facilities in the event of a network outage." Marconi Communications ("MD202") increases the cost efficiency by centralizing the management of switches: "A centrally managed, electronic distribution frame means that new users can be provisioned (or existing users reconfigured) remotely and quickly. This reduces manpower costs and also the operational risks associated with manual tasks in equipment rooms."

DCSs can switch DS1s and DS3s individually or multiplex them onto higher-bandwidth lines such as DS3s and optical lines. Multiplexing lower-capacity lines together onto higher-capacity lines results in lower costs. If the two endpoints of a dedicated leased line do not connect to the same central office, it is likely that the circuit will be multiplexed together with other circuits for some portion of its route. Because dynamic load balancing and dynamic routing also lead to lower costs, depending on the contractual agreement with the telephone company, the configuration and routing of the dedicated line may change sometimes in a manner that is transparent to the end user.

The differences in the security between dedicated leased lines and the PSTN are a result of how they are connected and who has access to them. Imaging this ill-conceived scenario (this is stupid – do not do it!): your PC at your office is connected to a dial-up modem that is configured to answer incoming calls. You have pcAnywhere running on your PC with no password. Your PC is connected to your network, to which you are connected as Administrator. This is a security nightmare by any measure. Nevertheless, if you keep your computer at home connected to this modem at all times, no one can dial in and take over your network because no one can make a connection.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

In the above scenario, if the dial-up line and modems are replaced with a dedicated leased line, the only fundamental difference is in what happens if the connection is broken. Using modems, if the connection is broken, someone else can dial in. Using a leased line, if the connection is broken, no one else can connect.

(The Internet presents a totally different issue with respect to connections. In general, using an Internet connection does not preclude others from using it simultaneously. No one will get a busy signal if he connects to your server via the Internet. Your Internet connection is available to anyone, from anywhere. Firewalls and other security measures must be used to control access.)

The lack of ubiquitous access to the end-points of a dedicated leased line is, in fact, the main feature that contributes to its security. Like many other aspects of network security, reducing exposure or opportunity improves the security of dedicated leased lines. An attacker who cannot connect cannot do any damage.

Unfortunately, the lack of ubiquitous access may not translate to the absolute lack of access. Physical access is one possibility. Another possibility is that some piece of equipment that is interposed in the circuit may be vulnerable.

Physical access may be possible at the end-user's wiring closet, at the telephone company's central office, and at any point in between – such as junction boxes and vaults. Physical access may be obtained surreptitiously or through the actions of an employee of the end-user or the telephone company. Once a tap is made, the attacker need only decode the signal into a usable data stream. While not trivial, there are no insurmountable obstacles in doing so.

Today's DCSs are usually managed remotely and have extensive capability for reconfiguration, testing and monitoring. Products are available that combine the functionality of PSTN switches and DCSs. If we are to treat dedicated leased lines as part of our trusted network, clearly we must also extend that trust to the vendor's equipment. The vendor's ability to manage leased-line infrastructure remotely using its IP network requires its customers to extend trust even further to its networks, employees, sub-contractors, and vendors. Can the telephone company's network be hacked? If so, can its switches be hacked? If so, do the switches provide the capability to capture your traffic? If you are satisfied with the answers to these questions today, what about next year?

Conclusions

Dedicated leased lines can be useful elements of a WAN and can contribute to the overall security of a network if their individual characteristics are understood and accounted for in consideration of overall security design. They are suitable for many applications, but they are not all the same; some are more dedicated than others. Because they share many characteristics with other types of service, they also may share lines and equipment with other types of service.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

You know your information is secure if you know that only you have access to it. Otherwise, you trust equipment, procedures, and people to maintain security for you. Ultimately, the degree to which you find the level of security to be acceptable depends on how important your information is and how well you have verified the trustworthiness of things not directly in your control. The chain of trust may include your employees, your vendors, your vendors' employees, your subcontractors, and your vendors' subcontractors.

Somewhere, someone, who is more interested in surfing the Internet than doing his job, might not change the default password for remotely accessing the new DCS.

Somewhere, someone, who does not have the proper training because of recent downsizing, might incorrectly reconfigure a circuit while attempting to do some routine maintenance.

Somewhere, someone, who has a huge gambling debt, might be willing to let your competitor eavesdrop on your circuit in exchange for making his problem go away before his wife finds out.

Effectively verifying the security of dedicated leased lines, to any degree of certainty, would be difficult and expensive. Most network professionals do not have the resources or the inclination to fully evaluate the security of their vendors. They would be wise, however, to look beyond the vendors' marketing claims and be aware of unseen issues that affect security. The safest choice is to not trust leased lines with protecting confidentiality of sensitive information. Encryption would provide a relatively simple, and inexpensive solution to effectively protecting confidentiality while taking advantage of the reliability and availability provided by dedicated leased lines.

Five points have been made:

- The concepts of "leased" and "dedicated," regarding WAN links, are contractually defined
- The facilities that connect the end-point locations of dedicated leased lines are not substantially different from those used in the PSTN
- The telephone company does not provide any guarantees with respect to security of the service unless the contract states that it does (the contract often states that it does not)
- The lack of ubiquitous access from the Internet contributes to security, but is not sufficient to guarantee security
- Securing the data may be more feasible than securing the line

Summary

In the effort to drive costs lower, the distinction between dedicated leased lines and other lines is increasingly becoming one of service-level guarantees. Dedicated leased lines are often justified solely because of their availability, reliability and capacity.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Viewing them as stand-alone, private, secure facilities, however, is naïve. They share many characteristics, and often facilities, with the PSTN infrastructure. Although difficult to compromise, in many ways they are not different from public switched facilities.

If these lines are to be used as part of a trusted network, the notion that they are inherently secure should be abandoned. Instead, a careful security evaluation should be undertaken, considering the specific configuration, connection points, equipment used, and the extent of access to the components of the line. The value of maintaining the confidentiality of the information to be transmitted should also be considered. The cost of a sufficient evaluation may be such that the less-expensive alternative is to not treat leased lines as part of the trusted network. In this case, confidentiality may be protected by using the same techniques that are used to secure information transmitted over public networks.

The decision of whether or not to trust dedicated leased lines with protecting the confidentiality of information must be based on knowledge of the details – not on myths or marketing claims.

References

"AT&T Business Communications Services Agreement", AT&T Business, URL: http://www.business.att.com/agreement/serviceagreement.jsp (25 April 2003)

"BellSouth® Long Distance Private Line Service", BellSouth Long Distance, Inc., 2002, URL: http://www.bellsouth.com/bsldcc/at_your_business/pdfs/privateLines.pdf (25 April 2003)

"Metro Private Line Services", MCI, URL: http://global.mci.com/us/enterprise/data/privatelines/metro/ (25 April 2003)

"Internet Services", Telenor Business Solutions, URL: www.telenorbusinessolutions.co.uk/services/internet_services/faqs/Leased%20Lines.html (25 April 2003)

"GENERAL TERMS AND CONDITIONS OF SERVICE", MCI, 2003, URL: http://global.mci.com/publications/service_guide/products/docs/g_general_terms_and_conditions.doc (25 April 2003)

"How Do We Convert an Analog Signal to a Digital Signal?", Lucent Technologies, 2002, URL: http://www.bell-labs.com/save/technology/common/64000bits.html (25 April 2002)

Lindner, Craig E., "Information Security Primer", 2001, URL: http://www.sans.org/rr/securitybasics/infosec_primer.php (25 April 2003)

© SANS Institute 2003, Author retains full rights.

Maillet, Edward (maillet@doc.cs.usm.maine.edu) “How secure is a WAN then?” [E-mail], 29 September 1995, URL: http://www.netssys.com/firewalls/firewalls-9509/0949.html (25 April 2003)

“MD202 Cross-Connect – for flexible, future-proof and profitable private and leased-line circuits”, Marconi Communications, 2000, URL: http://www.marconi.com/media/MD202_Bro.pdf (26 April 2003)

Nelson, R. A., “History Of Teletype Development”, Teletype Corporation, 1963, URL: http://www.thocp.net/hardware/history_of_teletype_development_.htm (25 April 2003)

“SCHEDULE NO. 7”, Sprint, 2002, URL: http://www.sprintbiz.com/customer_center/product_support/schedules/downloads/7tandc.pdf (25 April 2003)

“T1 Carrier -- The First Digital Transmission”, Lucent Technologies, 2002, URL: http://www.bell-labs.com/save/technology/common/t1carrier.html (25 April 2003)

“Working with T3 and T1: Technology, Troubleshooting and Fault Location”, Sunrise Telecom, Inc., URL: http://www.sunrisetelecom.com/technotes/T1-T3_book.pdf (26 April 2003)

© SANS Institute 2003, Author retains full rights.