Chapter 3

TEMPEST Secure Classified Local Area Networks

Computer Interconnect Systems

Hardwired systems often involve interconnecting a number of devices together such that they act as a network. Local Area Networks (LANs) are truly distributive processing systems. Basically, a LAN is a system of multiple processors and support equipment all sharing a common communications medium. Processors integrated in this way can immediately interchange information, plus any user can share the resources (printer, I/O device, etc.) of any other user on the net. When classified processing is involved in a distributed environment, either the environment is contained, or the information circulating through the environment is protected. Although encryption devices suitable for classified network applications are slowly becoming available, this section will discuss common solutions employed at this time.

Depending on the Government contractual requirements imposed, security of the net can be provided in the form of emission control, encryption, physical protection, or a combination of each. In many cases, the equipment of an entire facility is networked, with security requirements, including controlled access, imposed outside the building. Since normal commercial building practices do not easily lend themselves to network security measures, this section will concentrate on LAN protection as can be applied during or after installation of non-encrypted equipment in a commercial facility.

Distinguishing Features of Local Networks

Currently many acronyms describe computer networks. The Local Area Network (LAN) is the most popular, but networks are also called Local Computer Networks (LCN), Local Networks (LN), Local Area Computer Network (LACN), and Personal Computer Local Computer Network (PCLCN). Basically all these acronyms are describing the same technology: local communications technology.

For communications to take place between equipment, three basic requirements must be met. First, there must be some data rate at which communications can take place during transmission. For the personal computer network, the transmission rates involved are typically between 2.4 Kbps and 10 Mbps.

The second distinguishing characteristic for communications is the protected transmission media, the wire and cable over which signals are sent. For personal computer networks, twisted-pair cable and coaxial cable are the most popular, depending on the signal transmission rate and the size of the net. Typically, most LAN's extend from 100 feet to about 1 mile.

The third characteristic, and the primary distinguishing feature among the various network equipment suppliers, is the switching technology needed to switch from one point on the network to another. Protocols are a component of the switching mechanism used normally handled by hardware using VLSI technology. Protocols are the communications software, the software layered on top of the other network mechanisms.

Topologies

Two types of systems exist, open and closed. Open systems are essentially systems which are built or configured to a published specification or standard. Closed systems are completely proprietary, and require a formal gateway to interface into some other system. Various topologies, how the computers will be physically interconnected, have evolved for both open and closed system implementations. Figure 1 shows the common topology schemes for LAN's.

A star network has as its central element a server. Often used in voice/data applications, the switching technology employed in the star network resides at the center of the star, with all nodes located on the

perimeter. Since all communications go through the center of the star, TEMPEST requirements for the protection of unencrypted channels are necessary for this element.

In the majority of cases, TEMPEST suppression on the central element is not employed. The central element is usually located within a shielded enclosure, and individual nodes are located within a Secure Compartmented Information Facility (SCIF). However, unless all the individual personal computer nodes are located in a shielded area, and unless the wires connecting each node are physically and emission protected, there is a strong potential for compromise, either through crosstalk or through emissions outside the TEMPEST Protected Radiation Zone, to occur.

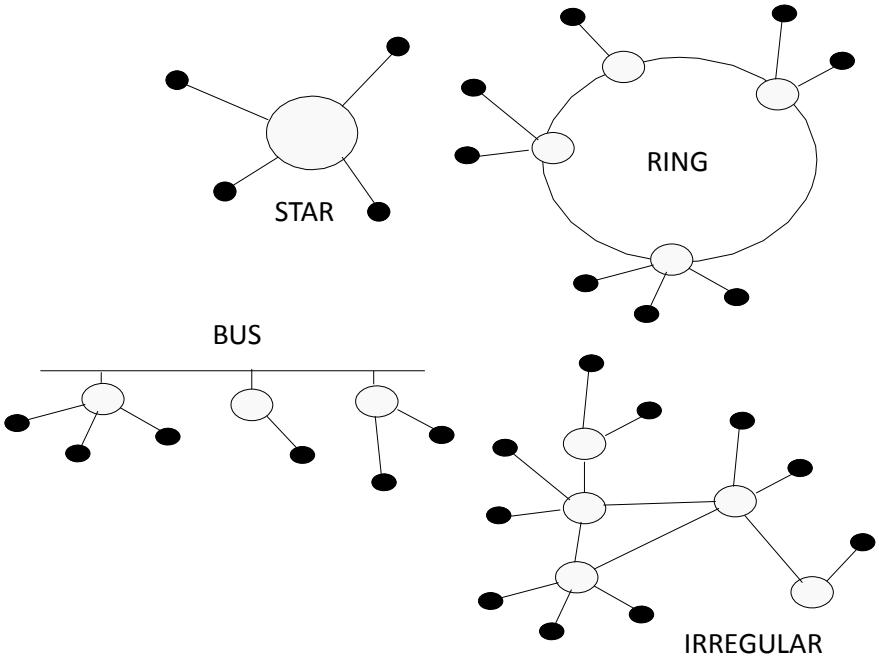


Figure 1 - Typical Hard-wired LAN Topologies

The ring network, or loop shown in Figure 1 has switching elements distributed along the ring, with nodes connecting to each element. The figure shows a system employing a common protocol technique called token passing. Instead of a bus contention scheme (listen before talking), some kind of token is used, and whoever has possession of the token actually gets to talk if they so desire.

The ring network is a more flexible system then the star, but is also much more difficult to TEMPEST protect. The primary problem relates to the distribution of the net. Again, unless encryption and TEMPEST techniques are employed at each node, the entire network must be located inside a SCIF and shielded from the outside world.

There are two other significant TEMPEST problems inherent with this topology. The first relates to distributed grounds. Since ground potentials differ at nearly every location along the ring, common mode ground loops are created among the various nodes connected, thus greatly reducing the emission controls implemented at each node. The condition is shown in Figure 2.

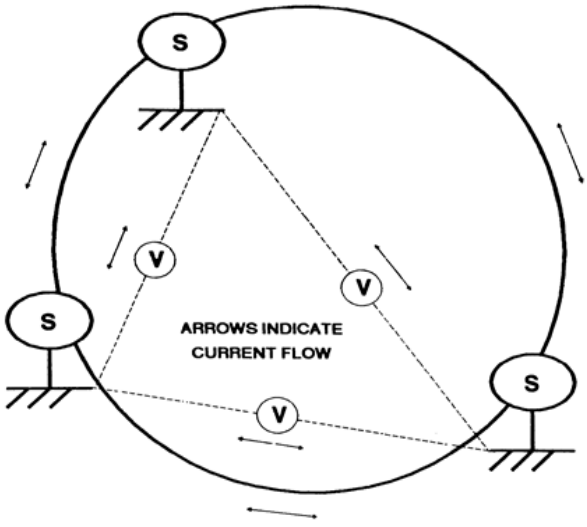


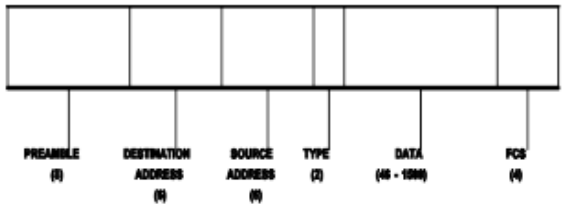
Figure 2 – Ring LAN Showing Ground Loops

The second problem relates to the twisted wire itself. Differential line drivers are prone to the effects of offset voltages. Therefore, twisted wire by itself does not reduce the transmitted signal sufficiently to eliminate radiated TEMPEST problems. In addition, since the ring might be large with several nodes, wave shaping and using shielded twisted pair might represent too much loss for the network to operate properly. Fiber optic cabling can eliminate the ground loop security problem with ring networks, but hardwired ring networks are seldom used in TEMPEST only security applications. The typical secure application with this approach is to employ encryption at terminals where security is desired.

The third popular LAN strategy is the bus. Branches are located at various points along the cable, as was shown in Figure 1. Of interest in this topology is the security capabilities and the generic (and ground controlled) interface using an interconnect control mechanism. Essentially, each node is independent, and can be connected or removed without effecting the other devices. Both TEMPEST secure and regular nodes can interface, inside and outside the shielded area. In addition, both fiber optic and TEMPEST secure coaxial cabling is available to support this form of topology, as are encrypting devices.

Ethernet Systems

Hardwired and fiber optic accredited Ethernet bus type systems are available and currently being used in a number of secure network applications. Ethernet systems employ a low-level access protocol which controls who actually gets control of the network at any one time. Called Carrier Sense Multiple Access, collision detection is used to handle contention (control) for the network. Basically, the node continually listens and waits until no one else is talking before it sends its message.



ETHERNET FRAME

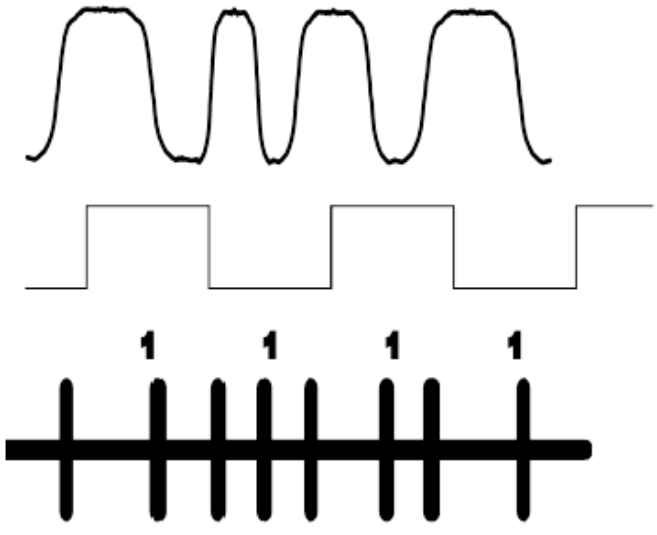


Figure 3 - Manchester Coding in Secure Ethernet LAN

On an Ethernet communications network, information is transmitted and received in Manchester encoded packets or frames. An Ethernet frame consists of a preamble, two address fields, a type field, an information field, and a frame check sequence. Each field has a specific format. An Ethernet frame has a minimum length of 64 bytes exclusive of the preamble, and a maximum length of 1518 bytes also exclusive of preamble. An Ethernet frame format is shown in Figure 3.

Of interest to the TEMPEST engineer is the encoding technique used to transmit data, the bandwidth requirements on the TEMPEST receiving system, and the inherent design of the Ethernet transmit circuitry.

Manchester encoding (or phase encoding) is a method of encoding the data in such a way that the clock signal can be

recovered from the serially transmitted data without the need of a separate clock channel. The idea is to introduce phase shifting in a carrier wave which is continuously switching, such that logic input changes are represented by a phase shift of the carrier. The transmitted signal is forced to make a transition at the center of each data bit. Logic "1" is transmitted by a 0 to 1 transition and "0" is transmitted by a 1 to 0 transition.

As an example, a high state 1 is encoded as a zero phase shift, with a low state represented by a 180 degree phase shift from reference. Two successive high or low states indicate either a positive or negative transition of the data input. Data resynchronization is achieved at the receiver by using a phase-locked loop that tracks the encoded signals.

The intended data and encoded signal was also shown in Figure 2. As can be seen, emission information related to state changes in Manchester encoded signals is more difficult to identify then with normal burst ASCII type coding.

A second difficulty in identifying Ethernet signals is the bandwidth requirements imposed on the equipment used to look at the signals. Since the burst pulses can be at 10 MHz rates, a wide bandwidth oscilloscope with memory is needed just to evaluate the signals that are radiated or conducted. Normally, a 400 MHz bandwidth memory scope is necessary.

The third advantage of Ethernet is the inherent harmonic control of the transmission circuitry. In order to prevent ringing along the entire cable length during a data and/or collision burst (the bus contention signal), the waveform's rise and fall characteristics have been suppressed about 80 db above the third harmonic. When the signal is transmitted over the coaxial cable, very little energy escapes to radiate to the outside world.

Classified LAN Security Philosophy

Whenever many individual devices are interconnected to form a network, the security of the entire network is much the same as the individual link in a chain. Any one component can cause a compromise, no matter how much protection is provided to the rest of the system. Referring back to the bus system of Figure 6.5, some pc's are connected to the system via a COMSEC access box. Since the data traversing the bus is encrypted, there would no system compromise as a result of signal line leakage or common-mode and ground loop coupling. However, unless the individual pc is also TEMPEST protected, the sensitive signals on the bus can still be detected in the vicinity of the receiving or transmitting pc interface.

Protecting the entire network involves the consideration of three design factors. First, each individual equipment in the network must be protected, either as a separate TEMPEST secure device, or through SCIF, vault, or building zone isolation. Second, unless fiber optic connections are used, the hardwire paths between each equipment must be protected by encrypting, emission shielding, or physical isolation (which could include facility shielding). The third factor involves the power and ground system used in the facility (see Figure 2).

LAN Security TEMPEST Verification

Related to non-COMSEC TEMPEST security, there are two common approaches to verifying the security of a Local Area Network. The first of these represents the application of NACSIM 5100A to both box and system level configurations. The objective with this approach is to satisfy TEMPEST criteria for an undetermined number of possible configurations with a discrete number of equipment and/or system level tests at a TEMPEST test laboratory prior to installation. Testing in this lower level configuration must consider ground loops and intra-system susceptibility for both test chamber measurements and field testing.

In order to meet TEMPEST objectives for initial test laboratory accreditation, the proper approach is to first perform scan testing to determine a worse case configuration prior to actual system level accreditation testing. Additionally, the underlying assumption for TEMPEST testing is that equipment to be accredited at the system level must first have met box level accreditation requirements.

The worst case configuration for lab testing should include at least one of each equipment type, should provide for a possible ground loop failure to occur between terminal interfaces or powerlines, should evaluate connector problems which might appear when the network equipment is improperly connected or removed, and should provide for the evaluation of possible standing waves and antenna effects along the transmission line. If the network is an Ethernet LAN, there is the requirement for grounding the coaxial cable at only one end if the network is to meet TEMPEST emission criteria.

The second philosophy for verifying the security of local area networks is to perform TEMPEST field tests after the network has been installed. When this approach is used, related security considerations such as the inherent shielding of the facility or location where the equipment is installed can enhance the protection otherwise provided by individual equipment.

Conclusion

Local Area Networks, particularly wireless, are true distributed processing communication system of the future. Secure networks, utilizing protected facilities, private security devices, COMSEC Type 1 or Type 2 devices, or TEMPEST emission controlled devices represent a major challenge to the TEMPEST design engineer related to grounding, power distribution, shielding, facility implementation, emission control, and systems integration. However, assuming all the proper TEMPEST design techniques have been implemented at the box and the overall facility level, there is still an element of uncertainty involved when putting the system together. This problem represents the final major challenge to the TEMPEST engineer who must certify the security of the system. The results and suggestions presented herein should aid in this effort.

References

Gabrielson, B.C., R & D Testing Ethernet Systems, Technical Report, Comsearch Applied Technology, Herndon, VA, 1985.

The Personal Computer Local Networks Report, Architecture Technology Corporation, Minneapolis, MN, 1985.