NETWORK TECHNOLOGIES FOR INFORMATION SECURITY PRACTITIONERS: PART 1

Chris Hare

INTRODUCTION

While it is common for security people to examine issues regarding network connectivity, there can be some level of mysticism associated with the methods and technologies that are used to actually construct the network. This article (see also [87-01-02]) addresses what a network is, and the different methods that can be used to build one. It also introduces issues surrounding the security of the network.

People send voice, video, audio, and data through networks. People use the Internet for bank transactions. People look up information in encyclopedias online. People keep in touch with friends and family using e-mail and video. As so much information is now conveyed in today's world through electronic means, it is essential that the security practitioner understands the basics of the network hardware used in today's computer networks.

PAYOFF IDEA

There is much about today's networking environments for the information security specialist to understand. However, being successful in assisting network engineers in designing a secure solution does not mean understanding all the components of the stack, or of the physical transport method involved. It does, however, require knowledge of what they are talking about and the differences in how the network is built with the different media options, and what the inherent risks are. The network designer and the security professional must have a strong relationship to ensure that the concerns for data protection and integrity are maintained throughout the network. Part 1 (this article) defines a network and discusses network devices and network topologies; and Part 2 (87-01-02) continues with network formats and cabling types.

WHAT IS A NETWORK?

A network is two or more devices connected together in such a way as to allow them to exchange information. When most people think of a network, they associate it with a computer network — ergo, the ability of two or more computers to share information among them. In fact, there are other forms of networks. Networks that carry voice, radio, or television signals. Even people establish networks of contacts — those people with whom they meet and interact.

In the context of this article, the definition is actually the first one — two or more devices that exchange information over some form of communications system.

NETWORK DEVICES

Network devices are computer or topology-specific devices used to connect the various network segments together to allow for data communication between different systems. Such devices include repeaters, bridges, routers, and switches.

Hubs

Hubs are used to concentrate a series of computer connections into one location. They are used with twisted pair wiring systems to interconnect the systems. Consider the traditional Ethernet network where each station is connected to a single network cable. The twisted pair network is unlike this; it is physically a star network. Each cable from a station is electrically connected to the others through a hub.

Hubs can be passive or active. A passive hub simply splits the incoming signal among all of the ports in the device. Active hubs retransmit the received signal into the other access ports. Active hubs support remote monitoring and support, while passive hubs do not.

The term “hub” is often extended to bridges, repeaters, routers, switches, or any combination of these.

Repeaters

A repeater retransmits the signal on one network segment to another segment with the original signal strength. This allows for very long networks when the actual maximum distance associated with a particular medium is not. For example, the 10base5 network standard allows for a maximum of four repeaters between two network stations. Because a coaxial segment can be up to 1500 meters, the use of the repeater significantly increases the length of the network.

Bridges

Bridges work by reading information in the physical data frames and determining if the traffic is for the network on the other side of the bridge. They are used in both Token Ring and Ethernet networks. Bridges filter the data they transmit from one network to another by only copying the frames that they should, based upon the destination address of the frame.

Routers

Routers are more sophisticated tools for routing data between networks. They use the information in the network protocol (e.g., IP) packet to determine where the packet is to be routed. They are capable of collecting and storing information on where to send packets, based on defined configurations or information that they receive through routing protocols. Many routers are only capable of two network connections, while larger scale routers can handle hundreds of connections to different media types.

Switches

A switch is essentially a multi-port bridge, although the term is now becoming more confusing. Switches have traditionally allowed for the connection of multiple networks for a certain length of time, much like a rotary switch. Two, and only two, networks are connected together for the required time period. However, today's switches not only incorporate this functionality, but they include routing intelligence to enhance their capability.

Network Types

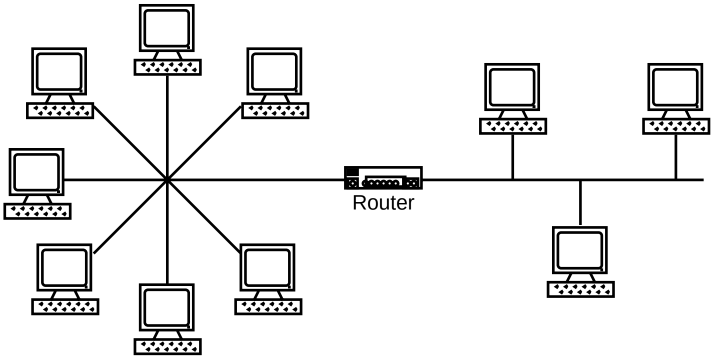
Networks can be large or small. Many computer hobbyists operate small, local area networks (LANs) within their own home. Small businesses also operate small LANs. Exactly when a LAN becomes something other than a LAN can be an issue for debate; however, a simpler explanation exists.

A LAN, as illustrated in Exhibit 1, connects two or more computers together, regardless of whether those computers are in the same room or on the same floor of a building. However, a LAN is no longer a LAN when it begins to expand into other areas of the local geography. For example, the organization that has two offices at opposite ends of a city and operates two LANs, one in each location. When they extend those two LANs to connect to each other, they have created a metropolitan area network (MAN); this is illustrated in Exhibit 2.

Note that a MAN is only applicable if two or more sites are within the same geographical location. For example, if the organization has two offices in New York City as illustrated in Exhibit 2, they operate a MAN. However, if one office is in New York and the other is in San Francisco (as shown in Exhibit 3), they no longer operate a MAN, but rather a WAN (i.e., wide area network).

These network layouts are combined to form inter-network organizations and establish a large collection of networks for information sharing.

EXHIBIT 1 — Sample Local Area Network



In fact, this is what the Internet is: a collection of local, metropolitan, and wide area networks connected together.

However, while networks offer a lot to the individual and the organization with regard to putting information into the hands of those who need it regardless of where they are, they offer some significant disadvantages.

It used to be that if people wanted to steal something, they had to break into a building, find the right desk or filing cabinet, and then physically remove something. Because information is now stored online, people have more information to lose, and more ways to lose it.

No longer do "burglars" need to break into the physical premises — they only have to find a way onto a network and achieve the same purpose. However, the properly designed and secured network offers more advantages to today's organizations than disadvantages.

However, a network must have a structure. That structure (or topology) can be as simple as a point-to-point connection, or as complicated as a multi-computer, multi-segment network.

NETWORK TOPOLOGIES

A network consists of segments. Each segment can have a specific number of computers, depending on the cable type used in the design. These networks can be assembled in different ways.

Point to Point

A point-to-point network consists of exactly two network devices, as seen in Exhibit 4. In this network layout, the two devices are typically connected via modems and a telephone line. Other physical media may

EXHIBIT 2 — Sample Metropolitan Area Network

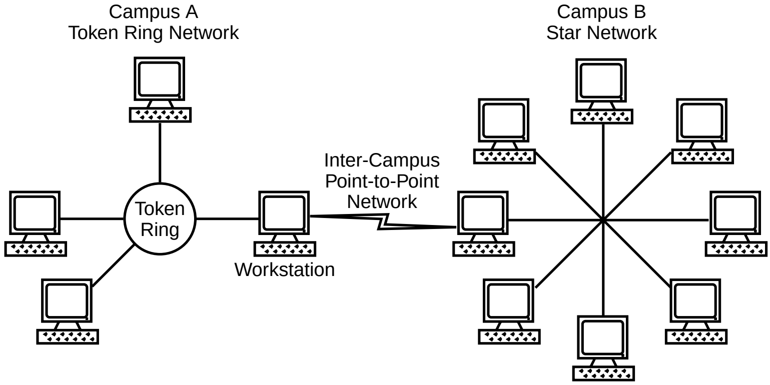
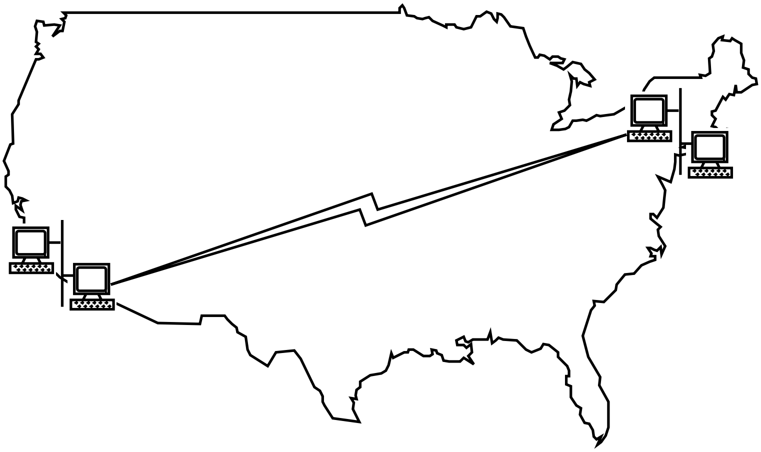


EXHIBIT 3 — Sample Wide Area Network



be used, for example twisted pair, but the applications outside the phone line are quite specific. In this type of network, the attacks are based at either the two computers themselves, or at the physical level of the connection. Because the connection itself can be carried by an analog modem, it is possible to eavesdrop on the sound and create a data stream that another computer can understand.

EXHIBIT 4 — Point-to-Point Network

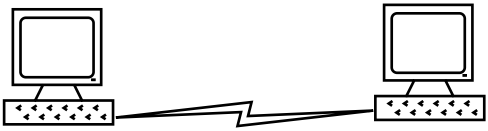
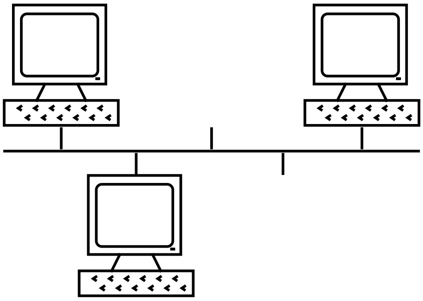


EXHIBIT 5 — Simple Bus Network



Bus

The bus network (see Exhibit 5) is generally thought of when using either 10base2 or 10base5 coaxial cabling. This is because the electrical architecture of this cabling causes it to form a bus or electrical length. The computers are generally attached to the cable using a connector that is dependent on cable type.

Bus networks can have a computer or network sniffer added on to them without anyone's knowledge as long as the physical limitations of the cabling have not been exceeded. If there is a spare, unused connector, then it is not difficult to add a network sniffer to capture network traffic.

Daisy Chain

The daisy-chain network as seen in Exhibit 6 is used in the thin-client or 10base2 coaxial network. When connecting stations in this environment, one can either create a point-to-point connection where systems are linked together using multiple dialup or point-to-point links, or connect station to station.

The illustration suggests that the middle station has two network cards. This is not the case, however; it was drawn in this exaggerated fashion to illustrate that the systems are *chained* together. In the case of

EXHIBIT 6 — Sample Daisy Chain Network

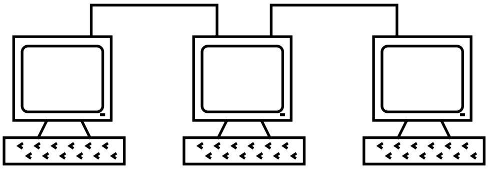
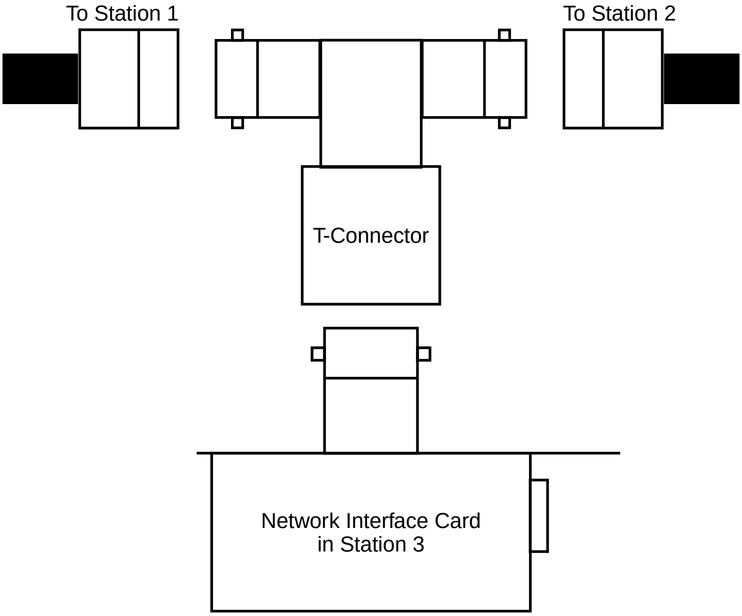


EXHIBIT 7 — Thin-Client Connections



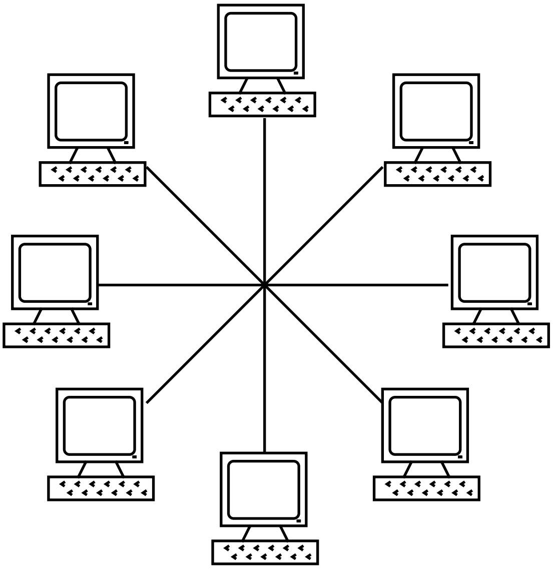
the thin-client network, the connections are made using two pieces of cable and a T-connector, which is then attached directly to the workstation, as shown in Exhibit 7.

This example illustrates how systems are daisy-chained, and specifically how it is accomplished with the 10base2 or thin-client network.

Star

Star networks (Exhibit 8) are generally seen in twisted pair type environments, in which each computer has its own connection or segment between it and the concentrator device in the middle of the star. All the connections are terminated on the concentrator that electrically links the cables together to form the network. This concentrator is generally called a hub.

EXHIBIT 8 — Simple Star Network



This network layout has the same issues as the bus. It is easy for someone to replace an authorized computer or add a sniffer at an endpoint of the star or at the concentrator in the middle.

Ring

The ring network (Exhibit 9) is most commonly seen in IBM Token Ring networks. In this network, a token is passed from computer to computer. No computer can broadcast a packet unless it has the token. In this way, the token is used to control when stations are allowed to transmit on the network.

However, while a Token Ring network is the most popular place to “see” a ring, a Token Ring network as illustrated in Exhibit 9 is electrically a star. A ring network is also achieved when each system only knows how to communicate with two other stations, but are linked together to form a ring, as illustrated in Exhibit 10. This means that it is dependent on those two other systems to know how to communicate with other systems that may be reachable.

EXHIBIT 9 — Token Ring Network

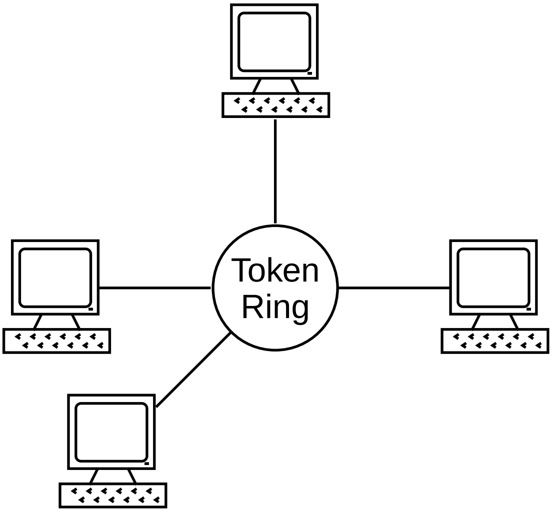
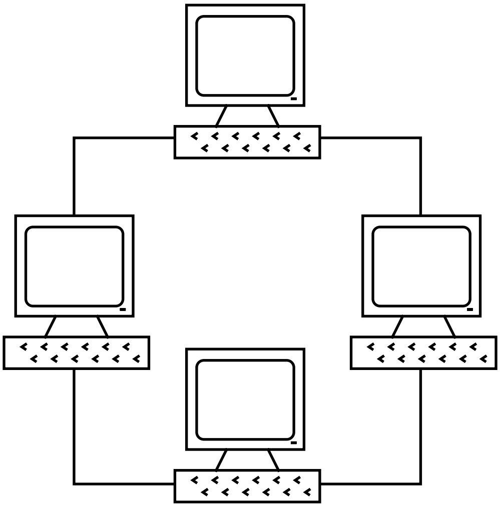


EXHIBIT 10 — Ring Network

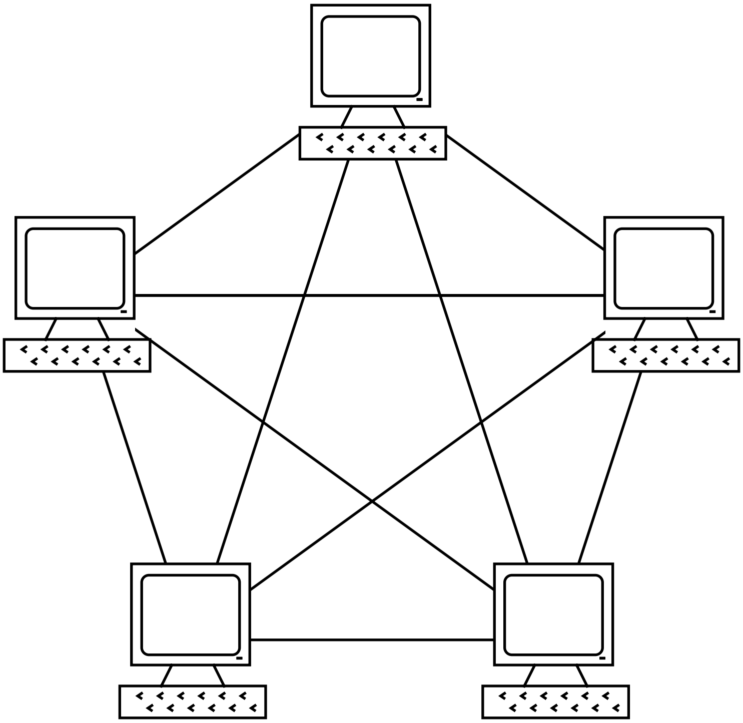


Auerbach Publications

Web

The web network (Exhibit 11) is complex and difficult to maintain on a large scale. It requires that each and every system on the network know how to contact any other system. The more systems in use, the larger and more difficult the configuration files. However, the web network has several distinct advantages over any of the previous networks.

EXHIBIT 11 — Web Network



It is highly robust, in that multiple failures will still allow the computer to communicate with other systems. Using the example shown in Exhibit 11, a single system can experience up to four failures. Even at four failures, the system still maintains communication within the web. The system must experience total communication loss or be removed from the network for data to not move between the systems.

This makes the web network extremely resilient to network failures and allows data movement even in high failure conditions. Organizations will choose this network type for these features, despite the increased network cost in circuits and management.

Each of the networks described previously relies on specific network hardware and topologies to exchange information. To most people, the exact nature of the technology used and the operation is completely transparent. And for the most part, it is intended to be that way.

Chris Hare, CISSP, lives in Ottawa, Canada, and is a senior systems security advisor with Nortel Networks Network & Computer Services. A noted speaker and author, he is a member of the (ISC)^2 Study Guide Development Committee and a part-time professor at Algonquin College (Ottawa, Canada) where he teaches information systems security courses.