TCP/IP is the primary protocol suite used on most networks and on the Internet. It is a robust protocol suite, but it has numerous security deficiencies.

Protocols that provide security services for application-specific communication channels are called secure communication protocols.

**Secure Communications Protocols**

**Simple Key Management for Internet Protocol (SKIP**) This is an encryption tool used to protect session less datagram protocols. SKIP was designed to integrate with IPSec; it functions at layer 3. It is able to encrypt any subprotocol of the TCP/IP suite. SKIP was replaced by Internet Key Exchange (IKE) in 1998.

**Software IP Encryption (swIPe)** This is another layer 3 security protocol for IP. It provides authentication, integrity, and confidentiality using an encapsulation protocol.

**Secure Remote Procedure Call (S-RPC)** This is an authentication service and is simply a means to prevent unauthorized execution of code on remote systems.

**Secure Sockets Layer (SSL**) This is an encryption protocol developed by Netscape to protect the communications between a web server and a web browser. SSL can be used to secure web, email, FTP, or even Telnet traffic. It is a session-oriented protocol that provides confidentiality and integrity. SSL is deployed using a 40-bit key or a 128-bit key. SSL is superseded by Transport Layer Security (TLS).

**Transport Layer Security (TLS)** TLS functions in the same general manner as SSL, but it uses stronger authentication and encryption protocols.

SSL and TLS both have the following features:

■ Support secure client-server communications across an insecure network while preventing tampering, spoofing, and eavesdropping.

■ Support one-way authentication.

■ Support two-way authentication using digital certificates.

■ Often implemented as the initial payload of a TCP package, allowing it to encapsulate all higher-layer protocol payloads.

■ Can be implemented at lower layers, such as layer 3 (the Network layer) to operate as a VPN. This implementation is known as OpenVPN.

In addition, TLS can be used to encrypt UDP and Session Initiation Protocol (SIP) connections. (SIP is a protocol associated with VoIP.)

**Secure Electronic Transaction (SET**) This is a security protocol for the transmission of transactions over the Internet. SET is based on Rivest, Shamir, and Adelman (RSA) encryption and Data Encryption Standard (DES). **It has the support of major credit card companies, such as Visa and MasterCard**. However, SET has not been widely accepted by the Internet in general; instead, SSL/TLS encrypted sessions are the preferred mechanism for secure e-commerce.

**Authentication Protocols**

After a connection is initially established between a remote system and a server or a network, the first activity that should take place is to verify the identity of the remote user. This activity is known as authentication. There are several authentication protocols that control how the logon credentials are exchanged and whether those credentials are

encrypted during transport:

**Challenge Handshake Authentication Protocol (CHAP)** This is one of the authentication protocols used over PPP links. **CHAP encrypts usernames and passwords**. It performs authentication using a challenge-response dialogue that cannot be replayed. CHAP also periodically reauthenticates the remote system throughout an established communication session to verify a persistent identity of the remote client. This activity is transparent to the user.

**Password Authentication Protocol (PAP)** This is a standardized authentication protocol for PPP. PAP transmits usernames and passwords in the clear. It offers no form of encryption; it simply provides a means to transport the logon credentials from the client to the authentication server.

**Extensible Authentication Protocol (EAP)** This is a framework for authentication instead of an actual protocol. EAP allows customized authentication security solutions, such as supporting smart cards, tokens, and biometrics.

**These three authentication protocols were initially used over dial-up PPP connections. Today, these and many other, newer authentication protocols and concepts are in use over a wide number of distance connection technologies, including broadband and virtual private networks (VPNs).**

**Protected Extensible Authentication Protocol (PEAP) encapsulates EAP in a TLS tunnel.** PEAP is preferred to EAP because EAP assumes that the channel is already protected but PEAP imposes its own security. PEAP is used for securing communications over 802.11 wireless connections. PEAP can be employed by Wi-Fi Protected Access (WPA) andWPA-2 connections.

PEAP is also preferred over Cisco’s proprietary EAP known as Lightweight Extensible Authentication Protocol (LEAP). LEAP was Cisco’s initial response to insecure WEP. LEAP supported frequent reauthentication and changing of WEP keys (whereas WEP used single authentication and a static key). However, LEAP is crackable using a variety of tools and techniques, including the exploit tool Asleap.

Secure Voice Communications

Normal private branch exchange (PBX) or POTS/PSTN voice communications are vulnerable to interception, eavesdropping, tapping, and other exploitations. Often, physical security is required to maintain control over voice communications within the confines of your organization’s physical locations. Security of voice communications outside your organization is typically the responsibility of the phone company from which you lease services. If voice communication vulnerabilities are an important issue for sustaining your security policy, you should deploy an encrypted communication mechanism and use it exclusively

**Voice over Internet Protocol (VoIP)**

VoIP is not without its problems. Hackers can wage a wide range of potential attacks against a VoIP solution:

■ Caller ID can be falsified easily using any number of VoIP tools, so hackers can perform vishing (VoIP phishing) or Spam over Internet Telephony (SPIT) attacks.

■ The call manager systems and the VoIP phones themselves might be vulnerable to host OS attacks and DoS attacks. If a device’s or software’s host OS or firmware has vulnerabilities, hacker exploits are often not far off.

Hackers might be able to perform man-in-the-middle (MitM) attacks by spoofing call managers or endpoint connection negotiations and/or responses.

■ Depending on the deployment, there are also risks associated with deploying VoIP phones off the same switches as desktop and server systems. This could allow for 802.1X authentication falsification as well as VLAN and VoIP hopping (i.e., jumping across authenticated channels).

■ Since VoIP traffic is just network traffic, it is often possible to listen in on VoIP communications by decoding the VoIP traffic when it isn’t encrypted.

**Social Engineering**

**Fraud and Abuse**

Another voice communication threat is PBX fraud and abuse. Many PBX systems can be exploited by malicious individuals to avoid toll charges and hide their identity. Malicious attackers known as phreakers abuse phone systems in much the same way that attackers abuse computer networks . Phreakers may be able to gain unauthorized access to personal voice mailboxes, redirect messages, block access, and redirect inbound and outbound calls. Countermeasures to PBX fraud and abuse include many of the same precautions you would employ to protect a typical computer network: logical or technical controls, administrative controls, and physical controls.

Manage Email Security

Clients retrieve email from their server-based inboxes using Post Office Protocol version 3 (POP3) or Internet Message Access Protocol (IMAP). Clients communicate with email servers using SMTP. Many Internet-compatible email systems **rely on the X.400 standard** for addressing and message handling.

**Sendmail is the most common SMTP server for Unix systems and Exchange is the most common SMTP server for Microsoft systems.**

**Secure Multipurpose Internet Mail Extensions (S/MIME)** Secure Multipurpose Internet Mail Extensions is an email security standard that offers authentication and confidentiality to email through public key encryption and digital signatures. Authentication is provided through X.509 digital certificates. Privacy is provided through the use of Public Key Cryptography Standard (PKCS) encryption. Two types of messages can be formed using S/MIME: signed messages and secured enveloped messages**. A signed message provides integrity, sender authentication, and nonrepudiation. An enveloped message provides integrity , sender authentication, and confidentiality.**

**MIME Object Security Services (MOSS)** MIME Object Security Services can provide authentication, confidentiality, integrity, and nonrepudiation for email messages. MOSS employs Message Digest 2 (MD2) and MD5 algorithms; Rivest, Shamir, and Adelman (RSA) public key; and Data Encryption Standard (DES) to provide authentication and encryption services.

**Privacy Enhanced Mail (PEM)** Privacy Enhanced Mail is an email encryption mechanism that provides authentication, integrity, confidentiality, and nonrepudiation. PEM uses RSA, DES, and X.509.

**DomainKeys Identified Mail (DKIM)** DKIM is a means to assert that valid mail is sent by an organization through

verification of domain name identity.

**Pretty Good Privacy (PGP)** Pretty Good Privacy (**PGP) is a public-private key system that uses** a variety of encryption algorithms to encrypt fi les and email messages. The first version of PGP used RSA, the second version, International Data Encryption Algorithm (IDEA), but later versions offered a spectrum of algorithm options. PGP is not a standard but rather an independently developed product that has wide Internet grassroots support.

Remote Access Security Management

Using a modem to dial up directly to a remote access server

■ Connecting to a network over the Internet through a VPN

■ Connecting to a terminal server system through a thin-client connection

**Dial-Up Protocols**

The two primary examples of dial-up protocols, PPP and SLIP, provide link governance, not only for true dial-up links but also for some VPN links:

**Point-to-Point Protocol (PPP)** This is a full-duplex protocol used for transmitting TCP/IP packets over various non-LAN connections, such as modems, ISDN, VPNs, Frame Relay, and so on. PPP is widely supported and is the transport protocol of choice for dial-up Internet connections. PPP authentication is protected through the use of various protocols, such as CHAP and PAP. PPP is a replacement for SLIP and can support any LAN protocol, not just TCP/IP.

**Serial Line Internet Protocol (SLIP)** This is an older technology developed to support TCP/IP communications over asynchronous serial connections, such as serial cables or modem dial-up. SLIP is rarely used but is still supported on many systems. It can support only IP, requires static IP addresses, offers no error detection or correction, and does not support compression

**Centralized Remote Authentication Services**

Centralized remote authentication services, such as RADIUS and TACACS+, provide this extra layer of protection. These mechanisms provide a separation of the authentication and authorization processes for remote clients that performed for LAN or local clients. The separation is important for security because if the RADIUS or TACACS+ servers are ever compromised, then only remote connectivity is affected, not the rest of the network.

**Remote Authentication Dial-In User Service (RADIUS)** This is used to centralize the authentication of remote dial-up connections. A network that employs a RADIUS server is configured so the remote access server passes dial-up user logon credentials to the RADIUS server for authentication. This process is similar to the process used by domain clients sending logon credentials to a domain controller for authentication.

**Terminal Access Controller Access-Control System (TACACS+)** This is an alternative to RADIUS. TACACS is available in three versions: original TACACS, Extended TACACS (XTACACS), and TACACS+. **TACACS integrates the authentication and authorization processes. XTACACS keeps the authentication, authorization, and accounting processes separate. TACACS+ improves XTACACS by adding two-factor authentication. TACACS+ is the most current and relevant version of this product line.**

Virtual Private Network

VPNs are most commonly associated with establishing secure communication paths through the Internet between two distant networks. However, they can exist anywhere, including within private networks or between end-user systems connected to an ISP. The VPN can link two networks or two individual systems. They can link clients, servers, routers, firewalls, and switches. VPNs are also helpful in providing security for legacy applications that rely on risky or vulnerable communication protocols or methodologies, especially when communication is across a network. VPNs can provide confidentiality and integrity over insecure or untrusted intermediary networks. They do not provide or guarantee availability. VPNs also are in relatively widespread use to get around location requirements for services like Netflix and Hulu and thus provide a (at times questionable) level of anonymity.

Tunneling

Regardless of the actual situation, tunneling protects the contents of the inner protocol and traffic packets by encasing, or wrapping, it in an authorized protocol used by the intermediary network or connection. Tunneling can be used if the primary protocol is not routable and to keep the total number of protocols supported on the network to a minimum.

tunneling is a point-to-point communication mechanism and is not designed to handle broadcast traffic. Tunneling also makes it difficult, if not impossible, to monitor the content of the traffic in some circumstances, creating issues for security practitioners.

Thus, traffic is unprotected within the source LAN, protected between the border VPN servers, and then unprotected again once it reaches the destination LAN.

**Common VPN Protocols**

**VPNs can be implemented using software or hardware solutions. In either case, there are four common VPN protocols: PPTP, L2F, L2TP, and IPSec. PPTP, L2F, and L2TP operate at the Data Link layer (layer 2) of the OSI model. PPTP and IPSec are limited for use on IP networks, whereas L2F and L2TP can be used to encapsulate any LAN protocol.**

**Point-to-Point Tunneling Protocol**

Point-to-Point Tunneling Protocol (PPTP) is an encapsulation protocol developed from the dial-up Point-to-Point Protocol. It operates at the Data Link layer (layer 2) of the OSI model and is used on IP networks. PPTP creates a point-to-point tunnel between two systems and encapsulates PPP packets. It offers protection for authentication traffic through the same authentication protocols supported by PPP:

■ Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)

■ Challenge Handshake Authentication Protocol (CHAP)

■ Password Authentication Protocol (PAP)

■ Extensible Authentication Protocol (EAP)

■ Shiva Password Authentication Protocol (SPAP)

**The initial tunnel negotiation process used by PPTP is not encrypted. Thus, the session establishment packets that include the IP address of the sender and receiver—and can include usernames and hashed passwords—could be intercepted by a third party. PPTP is used on VPNs, but it is often replaced by the L2TP, which can use IPSec to provide traffic encryption for VPNs. PPTP does not support TACACS+ and RADIUS.**

**Layer 2 Forwarding Protocol and Layer 2 Tunneling Protocol**

Cisco developed its own VPN protocol called Layer 2 Forwarding (L2F), which is a mutual authentication tunneling mechanism. However, L2F does not offer encryption. L2F was not widely deployed and was soon replaced by L2TP. As their names suggest, both operate at layer 2. Both can encapsulate any LAN protocol.

Layer 2 Tunneling Protocol (L2TP) was derived by combining elements from both PPTP and L2F. L2TP creates a point-to-point tunnel between communication endpoints. It lacks a built-in encryption scheme, but it typically relies on IPSec as its security mechanism**. L2TP also supports TACACS+ and RADIUS. IPSec is commonly used as a security mechanism for L2TP.**

**IP Security Protocol**

The most commonly used VPN protocol is now IPSec. IP Security (IPSec) is both a standalone VPN protocol and the security mechanism for L2TP, and it can be used only for IP traffic. IPSec works only on IP networks and provides for secured authentication as well as encrypted data transmission. IPSec has two primary components, or functions:

**Authentication Header (AH) AH provides authentication, integrity, and nonrepudiation.**

**Encapsulating Security Payload (ESP) ESP provides encryption to protect the confidentiality of transmitted data, but it can also perform limited authentication. It operates at the Network layer (layer 3)** and can be used in transport mode or tunnel mode. In transport mode, the IP packet data is encrypted but the header of the packet is not. In tunnel mode, the entire IP packet is encrypted and a new header is added to the packet to govern transmission through the tunnel.

Virtualization

Virtualization technology is used to host one or more operating systems within the memory of a single host computer. This mechanism allows virtually any OS to operate on any hardware. Such an OS is also known as a guest operating system. **From the perspective that there is an original or host OS installed directly on the computer hardware, the additional OSes hosted by the hypervisor system are guests**. It also allows multiple operating systems to work simultaneously on the same hardware. Common examples include VMWare, Microsoft’s Virtual PC, Microsoft Virtual Server, Hyper-V with Windows Server 2008, VirtualBox, and Apple’s Parallels.

**Virtual networking**

Software-defined networking (SDN) is a unique approach to network operation, design, and management. The concept is based on the theory that the complexities of a traditional network with on-device configuration (i.e., routers and switches) often force an organization to stick with a single device vendor, such as Cisco, and limit the flexibility of the network to adapt to changing physical and business conditions. SDN aims at separating the infrastructure layer (i.e., hardware and hardware-based settings) from the control layer (i.e., network services of data transmission management). Furthermore, this also removes the traditional networking concepts of IP addressing, subnets, routing, and the like from needing to be programmed into or be deciphered by hosted applications.

SDN offers a new network design that is directly programmable from a central location, is flexible, is vendor neutral, and is open standards based. Using SDN frees an organization from having to purchase devices from a single vendor. It instead allows organizations to mix and match hardware as needed, such as to select the most cost-effective or highest throughput–rated devices regardless of vendor. The configuration and management of hardware are then controlled through a centralized management interface. In addition, the settings applied to the hardware can be changed and adjusted dynamically as needed.

Another way of thinking about SDN is that it is effectively network virtualization. It allows data transmission paths, communication decision trees, and flow control to be virtualized in the SDN control layer rather than being handled on the hardware on a per-device basis.

Another interesting development arising out of the concept of virtualized networks is that of a virtual SAN (storage area network). A SAN is a network technology that combines multiple individual storage devices into a single consolidated network-accessible storage container. A virtual SAN or a software-defined shared storage system is a virtual re-creation of a SAN on top of a virtualized network or an SDN.

Network Address Translation

The goals of hiding the identity of internal clients, masking the design of your private network, and keeping public IP address leasing costs to a minimum are all simple to achieve through the use of network address translation (NAT). NAT is a mechanism for converting the internal IP addresses found in packet headers into public IP addresses for transmission

over the Internet .NAT was developed to allow private networks to use any IP address set without causing collisions or conflicts with public Internet hosts with the same IP addresses. In effect, NAT translates the IP addresses of your internal clients to leased addresses outside your environment.

NAT offers numerous benefits, including the following:

■ You can connect an entire network to the Internet using only a single (or just a few) leased public IP addresses.

■ You can use the private IP addresses defined in RFC 1918 in a private network and still be able to communicate with the Internet.

■ NAT hides the IP addressing scheme and network topography from the Internet.

■ NAT restricts connections so that only traffic stemming from connections originating from the internal protected network is allowed back into the network from the Internet. Thus, most intrusion attacks are automatically repelled.

**NAT is part of a number of hardware devices and software products, including firewalls, routers, gateways, and proxies. It can be used only on IP networks and operates at the Network layer (layer 3).**

**Private IP Addresses**

10.0.0.0–10.255.255.255 (a full Class A range)

172.16.0.0–172.31.255.255 (16 Class B ranges)

192.168.0.0–192.168.255.255 (256 Class C ranges)

**Stateful NAT**

NAT operates by maintaining a mapping between requests made by internal clients, a client’s internal IP address, and the IP address of the Internet service contacted. When a request packet is received by NAT from a client, it changes the source address in the packet from the client’s to the NAT server’s. This change is recorded in the NAT mapping database along with the destination address. Once a reply is received from the Internet server, NAT matches the reply’s source address to an address stored in its mapping database and then uses the linked client address to redirect the response packet to its intended destination. This process is known as stateful NAT because it maintains information about the communication sessions between clients and external systems

NAT can operate on a one-to-one basis with only a single internal client able to communicate over one of its leased public IP addresses at a time. This type of configuration can result in a bottleneck if more clients attempt Internet access than there are public IP addresses. For example, if there are only five leased public IP addresses, the sixth client must wait until an address is released before its communications can be transmitted over the Internet. Other forms of NAT employ **multiplexing techniques in which port numbers are used to allow the traffic from multiple internal clients to be managed on a single leased public IP address. Technically, this multiplexing form of NAT is known as port address translation (PAT) or overloaded NAT, but it seems that the industry still uses the term NAT to refer to this newer version**.

**Static and Dynamic NAT**

You can use NAT in two modes: static and dynamic.

**Static NAT** Use static mode NAT when a specific internal client’s IP address is assigned a permanent mapping to a specific external public IP address. This allows for external entities to communicate with systems inside your network even if you are using RFC 1918 IP addresses.

**Dynamic NA**T Use dynamic mode NAT to grant multiple internal clients access to a few leased public IP addresses. Thus, a large internal network can still access the Internet without having to lease a large block of public IP addresses. This keeps public IP address usage abuse to a minimum and helps keep Internet access costs to a minimum. In a dynamic mode NAT implementation, the NAT system maintains a database of mappings so that all response traffic from Internet services is properly routed to the original internal requesting client. Often NAT is combined with a proxy server or proxy firewall to provide additional Internet access and content-caching features.

NAT is not directly compatible with IPSec because it modifies packet headers, which IPSec relies on to prevent security violations. However, there are versions of NAT proxies designed to support IPSec over NAT. Specifically, NAT-Traversal (RFC 3947) was designed to support IPSec VPNs through the use of UDP encapsulation of IKE. IP Security (IPSec) is a standards-based mechanism for providing encryption for point-to-point TCP/IP traffic.

**Automatic Private IP Addressing**

Automatic Private IP Addressing (APIPA), aka link-local address assignment (defined in RFC 3927), assigns an IP address to a system in the event of a DHCP assignment failure.

APIPA is primarily a feature of Windows. APIPA assigns each failed DHCP client with an IP address from the range of 169.254.0.1 to 169.254.255.254 along with the default Class B subnet mask of 255.255.0.0. This allows the system to communicate with other APIPA configured clients within the same broadcast domain but not with any system across a router or with a correctly assigned IP address.

APIPA is not usually directly concerned with security. However, it is still an important issue to understand. If you notice that a system is assigned an APIPA address instead of a valid network address, that indicates a problem. It could be as mundane as a bad cable or power failure on the DHCP server, but it could also be a symptom of a malicious attack on the DHCP server. You might be asked to decipher issues in a scenario where IP addresses are presented. You should be able to discern whether an address is a public address, an RFC 1918 private address, an APIPA address, or a loopback address.

**Circuit Switching**

Circuit switching was originally developed to manage telephone calls over the public switched telephone network. In circuit switching, a dedicated physical pathway is created between the two communicating parties. Once a call is established, the links between the two parties remain the same throughout the conversation. This provides for fixed or known transmission times, a uniform level of quality, and little or no loss of signal or communication interruptions. Circuit switching systems employ permanent, physical connections. However, the term permanent applies only to each communication session. The path is permanent throughout a single conversation. Once the path is disconnected, if the two parties communicate again, a different path may be assembled. During a single conversation, the same physical or electronic path is used throughout the communication and is used only for that one communication. Circuit switching grants exclusive use of a communication path to the current communication partners. Only after a session has been closed can a pathway be reused by another communication.

**Packet Switching**

Eventually, as computer communications increased as opposed to voice communications, a new form of switching was developed. Packet switching occurs when the message or communication is broken up into small segments (usually fixed-length packets, depending on the protocols and technologies employed) and sent across the intermediary networks to the destination. Each segment of data has its own header that contains source and destination information. The header is read by each intermediary system and is used to route each packet to its intended destination. Each channel or communication path is reserved for use only while a packet is actually being transmitted over it. As soon as the packet is sent, the channel is made available for other communications. Packet switching does not enforce exclusivity of communication pathways. It can be seen as a logical transmission technology because addressing logic dictates how communications traverse intermediary networks between communication partners.

Circuit Switching Packet Switching

Constant traffic Bursty traffic

Fixed known delays Variable delays

Connection oriented Connectionless

Sensitive to connection loss Sensitive to data loss

Used primarily for voice Used for any type of traffic

In relation to security, there are a few potential issues to consider. A packet-switching system places data from different sources on the same physical connection. This could lend itself to disclosure, corruption, or eavesdropping. Proper connection management, traffic isolation, and usually encryption are needed to protect against shared physical pathway concerns. A benefit of packet-switching networks is that they are not as dependent on specific physical connections as circuit switching is. Thus, when or if a physical pathway is damaged or goes offline, an alternate path can be used to continue the data/packet delivery. A circuit-switching network is often interrupted by physical path violations.

**Virtual Circuits**

A virtual circuit (also called a communication path) is a logical pathway or circuit created over a packet-switched network between two specific endpoints. Within packet-switching systems are two types of virtual circuits:

■ Permanent virtual circuits (PVCs)

■ Switched virtual circuits (SVCs)

A PVC is like a dedicated leased line; the logical circuit always exists and is waiting for the customer to send data. A PVC is a predefined virtual circuit that is always available. The virtual circuit may be closed down when not in use, but it can be instantly reopened whenever needed. An SVC is more like a dial-up connection because a virtual circuit has to be created using the best paths currently available before it can be used and then disassembled after the transmission is complete. In either type of virtual circuit, when a data packet enters point A of a virtual circuit connection, that packet is sent directly to point B or the other end of the virtual circuit. However, the actual path of one packet may be different from the path of another packet from the same transmission. In other words, multiple paths may exist between point A and point B as the ends of the virtual circuit, but any packet entering at point A will end up at point B. A PVC is like a two-way radio or walkie-talkie. Whenever communication is needed, you press the button and start talking; the radio reopens the predefined frequency automatically (that is, the virtual circuit). An SVC is more like a shortwave or ham radio. You must tune the transmitter and receiver to a new frequency every time you want to communicate

with someone.

WAN Technologies

Technology Connection Type Speed

Digital Signal Level 0 (DS-0) Partial T1 64 Kbps up to 1.544 Mbps

Digital Signal Level 1 (DS-1) T1 1.544 Mbps

Digital Signal Level 3 (DS-3) T3 44.736 Mbps

European digital transmission format 1 El 2.108 Mbps

European digital transmission format 3 E3 34.368 Mbps

Cable modem or cable routers 10+ Mbps

Integrated Services Digital Network (ISDN) is a fully digital telephone network that supports both voice and high-speed data communications. There are two standard classes, or formats, of ISDN service.

**Basic Rate Interface (BRI)** offers customers a connection with two B channels and one D channel. The B channels support a throughput of 64 Kbps and are used for data transmission. The D channel is used for call establishment, management, and teardown and has a bandwidth of 16 Kbps. Even though the D channel was not designed to support data transmissions, a BRI ISDN is said to offer consumers 144 Kbps of total throughput.

**Primary Rate Interface (PRI**) offers consumers a connection with multiple 64 Kbps B channels (2 to 23 of them) and a single 64 Kbps D channel. Thus, a PRI can be deployed with as little as 192 Kbps and up to 1.544 Mbps. However, remember that those numbers are bandwidth, not throughput, because they include the D channel, which cannot be used for actual data transmission (at least not in most normal commercial implementations).

**WAN Connection Technologies**

Numerous WAN connection technologies are available to companies that need communication services between multiple locations and even external partners. These WAN technologies vary greatly in cost and throughput. However, most share the common feature of being transparent to the connected LANs or systems. A WAN switch, specialized router, or border connection device provides all the interfacing needed between the network carrier service and a company’s LAN. The border connection device is called the channel service unit/data service unit (CSU/DSU). These devices convert LAN signals into the format used by the WAN carrier network and vice versa. The CSU/DSU contains data terminal equipment/data circuit-terminating equipment (DTE/DCE), which provides the actual connection point for the LAN’s router (the DTE) and the WAN carrier network’s switch (the DCE). The CSU/DSU acts as a translator, a store-and-forward device, and a link conditioner. A WAN switch is simply a specialized version of a LAN switch that is constructed with a built-in CSU/DSU for a specific type of carrier network. There are many types of carrier networks, or WAN connection technologies, such as X.25, Frame Relay, ATM, and SMDS.

**X.25 WAN Connections**

X.25 is an older packet-switching technology that was widely used in Europe. It uses permanent virtual circuits to establish specific point-to-point connections between two systems or networks. It is the predecessor to Frame Relay and operates in much the same fashion. However, X.25 use is declining because of its lower performance and throughput rates when compared to Frame Relay or ATM.

**Frame Relay Connections**

Like X.25, Frame Relay is a packet-switching technology that also uses PVCs . However**, unlike X.25, Frame Relay supports multiple PVCs over a single WAN carrier service connectio**n. Frame Relay is a layer 2 connection mechanism that uses packet-switching technology to establish virtual circuits between communication endpoints. Unlike dedicated or leased lines, for which cost is based primarily on the distance between endpoints, Frame Relay’s cost is primarily based on the amount of data transferred. The Frame Relay network is a shared medium across which virtual circuits are created to provide point-to-point communications. All virtual circuits are independent of and invisible to each other.

A key concept related to Frame Relay is the committed information rate (CIR). The CIR is the guaranteed minimum bandwidth a service provider grants to its customers. It is usually significantly less than the actual maximum capability of the provider network. Each customer may have a different CIR established and defined in their contract. The service network provider may allow customers to exceed their CIR over short intervals when additional bandwidth is available. This is known as bandwidth on demand. (Although at first this might sound like an outstanding benefit, the reality is that the customer is charged a premium rate for the extra consumed bandwidth.) Frame Relay operates at layer 2 (the Data Link layer) of the OSI model as a connection-oriented packet-switching transmission technology.

Frame Relay requires the use of DTE**/DCE at each connection point. The customer owns the DTE, which acts like a router or a switch and provides the customer’s network with access to the Frame Relay network. The Frame Relay service provider owns the DCE**, which performs the actual transmission of data over the Frame Relay as well as establishing and maintaining the virtual circuit for the customer.

**ATM**

Asynchronous transfer **mode (ATM) is a cell-switching** WAN communication technology, as opposed to a packet-switching technology like Frame Relay. It fragments communications into fixed-length 53-byte cells. The use of fixed-length cells allows ATM to be very efficient and offer high throughputs. ATM can use either PVCs or SVCs. As with Frame Relay providers, ATM providers can guarantee a minimum bandwidth and a specific level of quality to their leased services. Customers can often consume additional bandwidth as needed when available on the service network for an additional pay-as-you-go fee. ATM is a connection-oriented packet-switching technology.

**SMDS**

Switched Multimegabit Data Service (SMDS) is a connectionless packet-switching technology. Often, SMDS is used to connect multiple LANs to form a metropolitan area network (MAN) or a WAN. SMDS was often a preferred connection mechanism for linking remote LANs that communicate infrequently. SMDS supports high-speed bursty traffic and bandwidth on demand. It fragments data into small transmission cells. SMDS can be considered a forerunner to ATM because of the similar technologies used.

**Specialized Protocols**

**Synchronous Data Link Control (SDLC)** Synchronous Data Link Control is used **on permanent physical connections** of dedicated leased lines to provide connectivity for mainframes, such as IBM Systems Network Architecture (SNA) systems. SDLC uses polling, operates at OSI layer 2 (the Data Link layer), and is a bit-oriented synchronous protocol.

**High-Level Data Link Control (HDLC)** High-Level Data Link Control is a refined version of SDLC designed specifically for serial synchronous connections. **HDLC supports full-duplex communications a**nd supports both point-to-point and multipoint connections. HDLC, like SDLC, uses polling and operates at OSI layer 2 (the Data Link layer). **HDLC offers flow control and includes error detection and correction.**

**High Speed Serial Interface (HSSI**) High Speed Serial Interface is a DTE/DCE interface standard that defines how multiplexors and routers connect to high-speed network carrier services such as ATM or Frame Relay. A multiplexor is a device that transmits multiple communications or signals over a single cable or virtual circuit. HSSI defines the electrical and physical characteristics of the interfaces or connection points and thus operates at OSI layer 1 (the Physical layer).

**Transparency**

Just as the name implies, transparency is the characteristic of a service, security control, or access mechanism that ensures that it is unseen by users. Transparency is often a desirable feature for security controls. The more transparent a security mechanism is, the less likely a user will be able to circumvent it or even be aware that it exists. With transparency, there is a lack of direct evidence that a feature, service, or restriction exists, and its impact on performance is minimal. In some cases, transparency may need to function more as a configurable feature than as a permanent aspect of operation, such as when an administrator is troubleshooting, evaluating, or tuning a system’s configurations.

**Verify Integrity**

To verify the integrity of a transmission, you can use a checksum called a hash total. A hash function is performed on a message or a packet before it is sent over the communication pathway. The hash total obtained is added to the end of the message and is called the message digest. Once the message is received, the hash function is performed by the destination system, and the result is compared to the original hash total. If the two hash totals match, then there is a high level of certainty that the message has not been altered or corrupted during transmission. Hash totals are similar to cyclic redundancy checks (CRCs) in that they both act as integrity tools. In most secure transaction systems, hash functions are used to guarantee communication integrity.

**Eavesdropping**

As the name suggests, eavesdropping is simply listening to communication traffic for the purpose of duplicating it.

**Impersonation/Masquerading**

Impersonation, or masquerading , is the act of pretending to b g e someone or something you are not to gain unauthorized access to a system.

**Replay Attacks**

Replay attacks are an offshoot of impersonation attacks and are made possible through capturing network traffic via eavesdropping. Replay attacks attempt to reestablish a communication session by replaying captured traffic against a system. You can prevent them by using one-time authentication mechanisms and sequenced session identification.

**Modification Attacks**

In modification attacks, captured packets are altered and then played against a system. Modified packets are designed to bypass the restrictions of improved authentication mechanisms and session sequencing. Countermeasures to modification replay attacks include using digital signature verifications and packet checksum verification.

**Hyperlink spoofing**

Hyperlink spoofing can take the form of DNS spoofing or can simply be an alteration of the hyperlink URLs in the HTML code of documents sent to clients. Hyperlink spoofing attacks are usually successful because most users do not verify the domain name in a URL via DNS; rather, they assume that the hyperlink is valid and

just click it…..