Wide Area Network Tips

WAN Media Facts

WANs can use one of several cable standards. When you contract for WAN services, you will need to understand your bandwidth needs to choose the appropriate cabling option. The table below describes common WAN carriers.

Carrier	Speed	Description
POTS	56 Kbps	• POTS stands for Plain Old Telephone Service, and is the wiring used for analog phone service • Existing wires use only one twisted pair • Analog signals are used through the local loop
T1	1.544 Mbps	• T-Carrier is a digital standard widely deployed in North America. • T1 lines usually run over two-pairs of unshielded twisted pair (UTP) cabling, although they can also run over other media such as coaxial, fiber-optic, and satellite. T3 lines usually run over fiber-optic cable. • A T1 line has 24 channels that each run at 64 Kbps. A T3 line has 672 channels that each run at 64 Kbps. • A T1/T3 connection requires a Channel Service Unit (CSU) and a Data Service Unit (DSU). (A DSU reads and writes synchronous digital signals, and a CSU manages the digital channel.)
T3	44.736 Mbps	
E1	2.048 Mbps	• E-Carrier is a digital standard very similar to T-Carrier, but it is widely deployed in Europe. • An E1 line has 32 channels that run at 64 Kbps. An E3 line transmits 16 E1 signals at the same time. • E1/E3 connections also require a CSU/DSU.
E3	34.368 Mbps	
J1	1.544 Mbps	• J-Carrier is a digital standard very similar to T-Carrier, but it is widely deployed in Japan. • A J1 line is virtually identical to a T1 line. A J3 line has 480 channels that run at 32 Mbps. • J1/J3 connections also require a CSU/DSU.
J3	32.064 Mbps	
OC-1	51.84 Mbps	• Optical carrier specifications define the types and throughput of fiber optic cabling used in SONET (Synchronous Optical Network). • Each OC level is a multiple of the Base Rate (OC-1). To get the 622.08 Mbps throughput rating of OC-12, multiply the 51.84 Mbps Base Rate by 12.
OC-3	155.52 Mbps	
OC-12	622.08 Mbps	
OC-24	1244.16 Mbps	
OC-48	2488.32 Mbps	
OC-192	10 Gbps	
OC-256	13.271 Gbps	
OC-768	39.2 Gbps	

WAN Facts

A generic wide area network uses the following components:

Component	Description
WAN cloud	The WAN cloud is the collection of equipment that makes up the WAN network. The WAN cloud is owned and maintained by large telecommunications companies. It is represented as a cloud because the physical structure varies, and different networks with common connection points may overlap. Few people thoroughly understand where data goes as it is switched through the "cloud." What is important is that data goes in, travels through the line, and arrives at its destination.
Central Office (CO)	The central office is a switching facility connected to the WAN, and is the nearest point of presence for the WAN provider. It provides WAN-cloud entry and exit points.
Local loop	The local loop is the cable that extends from the central office to the customer location. The local loop is owned and maintained by the WAN service provider. Typically, it is UTP, but it can also be one or a combination of UTP, fiber optic, or other media. The local loop is often referred to as the "last mile" because it represents the last portion of the WAN up to the customer premises.
Demarcation point (demarc)	When you contract with a local exchange carrier (LEC) for data or telephone services, they install a physical cable and a termination jack onto your premises. The demarcation point is the line that marks the boundary between the telco equipment and the private network or telephone system. • Typically, the LEC is responsible for all equipment on one side of the demarc, and the customer is responsible for all equipment on the other side of the demarc. • The demarc is also called the minimum point of entry (MPOE) or the end user point of termination (EU-POT). • The demarc is typically located in the bottom floor of a building, just inside the building. For residential service, the demarc is often a small box on the outside of the house.
Consumer Premises Equipment (CPE)	Devices physically located on the subscriber's premises are referred to as the consumer (or customer) premises equipment. CPE includes the telephone wire, telephone, modem, and other equipment, both the devices the subscriber owns and the ones leased from the WAN provider.
Channel Service Unit/Data Service Unit (CSU/DSU)	A CSU/DSU is a device that converts the signal received from the WAN provider into a signal that can be used by equipment at the customer site. A CSU/DSU is composed of two separate devices: • The CSU terminates the digital signal and provides error correction and line monitoring. • The DSU converts the digital data into synchronous serial data for connection to a router. The CSU/DSU might be two separate devices, one combined device, or it might be integrated into a router.

WANs employ one of the two following methods to transfer data:

Method	Description
Circuit Switching	A circuit switched network uses a dedicated connection between sites. Circuit switching is ideal for transmitting data that must arrive quickly in the order it is sent, as is the case with real-time audio and video.
Packet Switching	A packet switched network allows data to be broken up into packets. Packets are transmitted along the most efficient route to the destination. Packet switching is ideal for transmitting data that can handle transmission delays, as is often the case with Web pages and e-mail.

WAN Services Facts

The following table describes common WAN services that are used to connect two networks through a WAN.

Service	Description
Public Switched Telephone Network (PSTN)	The PSTN is the network used for placing local and long-distance phone calls. • The PSTN is a circuit switched network; a dedicated circuit is established when the call is placed and remains in place throughout the call. • The local loop uses analog signals over POTS (regular telephone cable wires). The long-distance network typically uses digital signaling over fiber optic. • End-to-end speeds are limited to 56 Kbps, a limitation imposed by the limitations of POTS in the local loop at each end. • A modem is required to convert digital signals to analog. • The PSTN is used by remote access clients to access the network, or as a temporary or backup connection between sites.
Integrated Services Digital Network (ISDN)	Integrated Services Digital Network (ISDN) is a WAN technology that provides increased bandwidth within the local loop. There are two forms of ISDN: • ISDN BRI (basic rate interface) uses digital signals over POTS. The traditional phone line is divided into separate channels: two 64 Kbps bearer (B) channels and one 16 Kbps control (D) channel. ISDN BRI is often called 2B + 1D. • ISDN PRI (primary rate interface) uses digital signals over a T1 line with 23 64 Kbps B channels and one 64 Kbps D channel in North America (up to 1.544 Mbps), or over an E1 line with 30 64 Kbps B channels and one 64 Kbps D channel (up to 2.048 Mbps). ISDN PRI is often referred to as 23B + 1D. ISDN has the following characteristics: • ISDN is a circuit switching technology. • ISDN is only a local loop technology; once calls reach the WAN cloud, they are converted to another protocol for transmission through the WAN. • With ISDN BRI, you can use one channel for voice and one channel for data, or both channels for different voice calls. Depending on the implementation, you can also bond both B channels to use them together. • ISDN PRI requires a CSU/DSU for the T1 line.

Frame Relay	Frame Relay is a protocol used to connect to a WAN over dedicated (leased) lines.
	
	• Frame Relay is a packet switching technology that supports variable-sized data units called *frames*.
	• Frame Relay establishes a permanent virtual circuit between two locations. This circuit is virtual, meaning it is not a physical path through the network. Because the circuit is permanent, there is no call setup or termination required.
	• Virtual circuits can be configured as one of the following:
	  ○ A point-to-point circuit is established between two locations.
	  ○ A point-to-multipoint circuit is a single circuit that can be used to reach multiple locations.
	• Frame Relay can be implemented over a variety of connection lines (T1, T3).
	• Routers at the customer site connect to the T1 line through a CSU/DSU.
	• When congestion occurs, the Frame Relay network simply drops packets to keep up. Frame Relay networks provide error detection but not error recovery. It is up to end devices to request a retransmission of lost packets.
	• When you sign up for Frame Relay service, you are assigned a level of service called a Committed Information Rate (CIR). At times your actual bandwidth could be higher than the CIR, but the CIR represents the maximum *guaranteed* data transmission rate you will receive on the Frame Relay network.

Asynchronous Transfer Mode (ATM)	ATM is a WAN communication technology originally designed for carrying time-sensitive data such as voice and video. However, it can also be used for regular data transport.
	
	• ATM is a packet switching technology that uses fixed-length data units called *cells*. Each cell is 53-bytes.
	• ATM establishes a virtual circuit between two locations.
	  ○ A virtual *channel* is a data stream sent from one location to another.
	  ○ A virtual *path* is a collection of data streams with the same destination.
	• The cell header includes labels that identify the virtual path information. ATM switches in the WAN cloud use the virtual path to switch cells within the WAN to the destination.
	• ATM is connection-oriented (compared to Frame Relay which is connectionless).

Synchronous Optical Networking (SONET)	SONET is a subset or variation of the Synchronous Digital Hierarchy (SDH) standards for networking over an optical medium. It was originally developed as a WAN solution to interconnect optical devices from various vendors. • SONET is a packet switching technology that uses different frame sizes based on the bandwidth used on the SONET network. • SONET is classified as a transport protocol, in that it can carry other types of traffic such as ATM, Ethernet, and IP. • Most PSTN networks use SONET within the long-distance portion of the PSTN network. • SONET networks use dual, counter-rotating fiber optic rings. If a break occurs in one ring, data can be routed over the other ring to keep traffic flowing.

	• Data rates for SONET vary from between 51 Mbps up to about 160 Gbps.
Multiprotocol Label Switching (MPLS)	MPLS is a WAN data classification and data carrying mechanism. • MPLS is a packet switching technology that supports variable-length frames. • MPLS adds a label to packets between the existing Network and Data Link layer formats. Labels are added when the packet enters the MPLS network, and removed when the packet exits the network. • Information in the label is used to switch the packet through the MPLS network to the destination. • MPLS labels can identify the route or even the network type to use. MPLS labels are often used to provide different classes of service for data streams. • MPLS is a connection-oriented protocol.

Internet Services Facts

Internet connectivity provides methods (sets of standards) that allow computers to connect to the Internet through an ISP. The two primary methods of Internet connection are through dialup or LAN.

Method	Description
Public Switched Telephone Network (PSTN)	The PSTN uses a single POTS (Plain Old Telephone Service) phone line with a modem. • Dial-up uses a single 64 Kbps channel. • Common data transfer rates include 28.8 Kbps, 33.3 Kbps, and 56 Kbps. • Dial-up offers sufficient network connectivity for a minimal investment. It is available virtually anywhere that regular voice grade communications are available. • Computers dial an access server at the ISP. Configuration requires the ISP server's phone number, along with a username and password to log on). • The phone line *cannot* be used for voice and the Internet concurrently.

Digital Subscriber Line (DSL)	DSL offers digital communications over existing POTS lines.
	
	• Data is sent in multiple channels over existing wiring.
	• Configuration requires a DSL router (or a cable modem) or NIC attached (with USB or Ethernet) to the phone line.
	• DSL is not available everywhere; the location must be within a fixed distance of network switching equipment.
	
	There are multiple variations of DSL (collectively referred to as xDSL). Variations included:
	
	• Asymmetrical DSL (ADSL) provides different download and upload speeds.
	  ○ Speeds are up to 12 Mbps downstream and 1-3.5 Mbps upstream. Newer ADSL2+ provides up to 24 Mbps downstream.
	  ○ ADSL allows regular analog dial-up and digital access on the same line at the same time. Splitters are required to keep the analog signals from interfering with the digital signals.
	  ○ ADSL is good for Internet access (browsing), but is not well suited if you

	need to provide Internet services (such as maintaining your own Web site).
	• Symmetrical DSL (SDSL) provides equal download and upload speeds.
	  ○ Depending on the region, speeds are between 1.544-2.048 Mbps. Newer SHDSL provides between 4.6-5.696 Mbps.
	  ○ The entire line is used for data; simultaneous voice and data is *not* supported. Splitters are not required because voice traffic does not exist on the line.
	• Very high DSL (VDSL or VHDSL) is similar to asymmetrical DSL with higher speeds.
	  ○ Speeds can be up to 52 Mbps downstream and 12-16 Mbps downstream, depending on the distance. Newer VDSL2 provides up to 100 Mbps at a distance of 300 meters.
	  ○ Both voice and digital data is supported on the same line at the same time; splitters are required.

Integrated Services Digital Network (ISDN)	ISDN offers digital communications over either existing POTS lines or T1 lines. • ISDN is more common in Europe than in the United States. • The transmission medium is divided into channels for digital data. • Subscribers must be within a certain distance of the phone company equipment, although this distance can be extended with repeaters. • Phone calls use digital ISDN phones, or analog phones connected to a converter. There are two main implementations of ISDN: • ISDN BRI (basic rate) provides two 64 Kbps channels for data and one 16 Kbps control channel. BRI uses 4 wires on the existing POTS installation. With ISDN BRI, you can use one channel for voice and one channel for data, or both channels for different voice calls. Depending on the implementation, you can also bond both B channels to use them together for faster data speeds. • ISDN PRI (primary rate) provides 23 64 Kbps data channels and one 64 Kbps control channel on a T1 line (or 30 data channels on an E1 line).
Cable	Cable Internet access is typically offered by companies that provide cable television access. Existing cable TV lines provide bandwidth for Internet access in addition to cable TV stations. • Cable Internet uses a cable modem to convert analog signals over multiple channels. • Speeds can be up to 30 Mbps, but bandwidth is shared between users within the same area (neighborhood). Actual speeds may be much less than the maximum. • Many cable providers prevent you from connecting more than a single host to the network.
Satellite	Satellite provides Internet access through signals received from orbiting satellites. • Satellite service providers offer nearly 100% global network coverage (a local network infrastructure is unnecessary). Satellite is often available even when other forms or access are not (DSL or even dial-up).

	• A local portable transmitter with an antenna (dish), along with direct line of sight (no obstructions) with satellites is required. • Satellite reception is subject to mild atmospheric and weather conditions (fog or slight wind can disrupt service). • Many services only allow for satellite downloading (very fast). A POTS modem may be required to upload (very slow).
Wireless	Wireless access is typically available at local businesses, either free or for a fee. In addition, many city and residential areas have coverage from a wireless Internet provider. • Some providers offer a nation-wide network of wireless access points in common public locations, such as airports. Signing up for this service might make sense for frequent travelers. • Wireless networks set up in downtown areas allow limited roaming (moving) within the area of coverage. However, some dead spots might limit access. • Wireless networks in residential areas are best suited for stationary clients.

Remote Access Facts

Remote access allows a host to connect remotely to a private server or a network to access resources on that server or network. Remote access connections are typically used to connect remotely to servers at your office, but can also describe the type of connections used to connect to an Internet Service Provider (ISP) for Internet access. A remote access server is a server configured to allow remote access connections.

The following process is used to establish a remote access connection.

Process	Description
Physical connection	As a first step, clients must establish a physical connection to the remote access server. • For dialup clients, this process includes getting a dial tone, dialing the number of the remote access server, and having the remote access server answer the incoming call. • For clients with a broadband or always on connection, the connection is established when you connect the device to the network and turn it on.
Connection parameters	After the physical connection is established, a Data Link layer connection is established. During this phase, additional parameters that will be used during the connection are established. For example, the devices identify the upper-layer protocols that they will use during the connection. Protocols negotiated at this phase control: • Upper-layer protocol suite (such as IP) • Network-layer addressing • Compression (if any) • Encryption (if any) • The authentication method to use Two common protocols used during this phase are:

	• The Point-to-Point Protocol (PPP) is used for dial-up connections. • PPP over Ethernet (PPPoE) is used for connections that have an "always on" state, such as DSL or fiber optic running Ethernet. PPPoE is a modification of PPP that allows for negotiation of additional parameters that are typically not present on a regular Ethernet network. ISPs typically implement PPPoE to control and monitor Internet access over broadband links. During this phase, one of the things to happen is that the remote client is assigned an IP address. The IP address can be assigned from a range configured on the remote access server, or even from a DHCP server on the private network. • If the IP address for the remote client is on the same subnet as the private network, the remote access server uses a process called *proxy ARP* to forward packets from the private network to the remote access client. With proxy ARP, the MAC address of the remote access server is associated with the IP address of the remote clients. The remote access server receives the frames addressed to the remote access client, and forwards the packets to the remote access client. • If the IP address for the remote client is on a different subnet, for example a special subnet defined for remote access clients, then the remote access server acts as a router sending packets between the remote client and the public network. In this configuration, the remote access server must be configured with routing enabled.
Authentication	*Authentication* is the process of proving identity. The authentication protocol is negotiated during the connection parameter phase. After devices agree on the authentication protocol to use, the logon credentials are exchanged and logon is allowed or denied. Common protocols used for remote access authentication include: • Challenge Handshake Authentication Protocol (CHAP) • Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) • Extensible Authentication Protocol (EAP) Both CHAP and MS-CHAP are used for username and password authentication, while EAP allows authentication using a variety of methods including passwords, certificates, and smart cards.
Authorization	*Authorization* is the process of identifying the resources that a user can access over the remote access connection. Authorization can restrict access based on: • Time of day • Type of connection (e.g. PPP or PPPoE, wired or wireless) • Location of the resource (i.e. restrict access to specific servers)
Accounting	*Accounting* is an activity that tracks or logs the use of the remote access connection. Accounting is often used by ISPs to bill for services based on time or the amount of data downloaded.

Be aware of the following with remote access.

- The remote access server controls access for remote access clients. Clients might be restricted to access only resources on the remote access server, or might be allowed access to resources on other hosts on the private network.
- Both the remote access server and the client computers must be configured to use or accept the same connection parameters. During the connection phase, the devices negotiate the protocols that will be used. If the allowed protocols do not match, the connection will be refused.
- Remote access policies identify allowed users and other required connection parameters.
- In a small implementation, user accounts and remote access policies are defined on the remote access server.
- When using a directory service, you can configure the remote access server to look up user account information on the directory service server.
- If you have multiple remote access servers, you must define user accounts and policies on each remote access server.
- Use an AAA server to centralize authentication, authorization, and accounting for multiple remote access servers. Connection requests from remote clients are received by the remote access server and forwarded to the AAA server to be approved or denied. Policies defined on the AAA server apply to all clients connected to all remote access servers.
- Two common AAA server solutions include:

Solution	Description
Remote Authentication Dial-In User Service (RADIUS)	RADIUS is used by Microsoft servers for centralized remote access administration. RADIUS: ○ Combines authentication and authorization using policies to grant access. ○ Uses UDP. ○ Encrypts only the password. ○ Often uses vendor-specific extensions. RADIUS solutions from different vendors might not be compatible. When configuring a RADIUS solution, configure a single server as a RADIUS server. Then configure all remote access servers as RADIUS clients.
Terminal Access Controller Access-Control System Plus (TACACS+)	TACACS+ was originally developed by Cisco for centralized remote access administration. TACACS+: ○ Provides three protocols, one each for authentication, authorization, and accounting. This allows each service to be provided by a different server. ○ Uses TCP. ○ Encrypts the entire packet contents. ○ Supports more protocol suites than RADIUS.