Learn, network and share

Read about this year's TCUK conference

Communicator

The Institute of Scientific and Technical Communicators
Winter 2015

Localise content through web design

The world of analytical engineering

Learn more about networks

Are technical communicators grumpy?

An introduction to networks

Warren Singer and Wael Elazab discuss the relevance of networks to technical communication.

Introduction

Welcome to the Technology column. This column is written by a team of contributors with the aim of describing technology that is relevant to technical communicators. The purpose is to explain what the technology is, why it is relevant, and provide background information and links where you can find out more.

The backbone of the Internet consists of fibre-optic cables running across continents and between continents

What are networks?

Networks are all around us. The best example of a network is the Internet. We tend to think of the Internet as a type of ether, a magical way of transporting data from anywhere to anywhere else. But behind all of this magic lies a vast physical infrastructure.

The 'Internet' is made up of a number of global networks that are connected with each other in a gigantic web of copper and fibre-optic cables that run across continents and beneath oceans like a huge spider web, criss-crossing and intersecting.

For many of us technical communicators, a basic understanding of networks is necessary, because so many of the products and applications that we are asked to document or use run over a network infrastructure.

But how do networks like the Internet actually work? How is data transferred from one machine to another? An understanding of the fundamentals of networking can add value to your role as a technical communicator, when talking with developers, testers, architects or IT staff, and when documenting services or systems that reside within a network.

"Everything you do online travels through a tube. Inside those tubes by and large are glass fibres. Inside those fibres is light. Encoded in that light is, increasingly, us," (Blum, 2012)

Tubes

In his book Tubes, Andrew Blum describes the Internet as consisting of a network of tubes (Blum, 2012).

The backbone of the Internet runs on fibre-optic cables, each capable of carrying data, in the form of light pulses (Gibson, 2011). Repeaters are interspersed at intervals to ensure the signal is boosted and not lost. Fibre-optic technology provides the scalability and speed necessary to ensure sufficient bandwidth is available for the enormous processing needs of today's Internet.

These long-distance cables are laid by networking companies, which run them across continents and under oceans. Fibre-optic cables have replaced or supplemented the original transatlantic telephone cables that connected countries such as the United States by wire to Europe. Undersea fibre-optic cables connect to large port cities such as Lisbon, Marseilles, Hong Kong, Singapore, New York and Alexandria. Porthcurno, near Lands End, is the biggest intercontinental route between New York and London and several important cables pass through it (Blum, 2012).

Internet exchanges

The fibre-optic cables are connected via internet exchanges, into which different network providers can plug their networks to enable interconnectivity to other networks. Examples of such exchanges include MAE-EAST in Chicago, the Palo Alto Internet Exchange in Silicon Valley, Equinix in Ashburn, USA and Docklands in Canary Wharf, UK. Fibre-optic cable runs under the A13 and into Telehouse in Canary Wharf. Major companies can then connect to the fibre-optic network by running their own cables into Telehouse or installing equipment onsite at Telehouse (Blum, 2012).

Internet exchanges and peering

Internet exchanges such as those in London, Amsterdam and Frankfurt bid for networking companies to connect through them (Blum, 2012).

Making connections between networks (via internet exchanges) is known as peering. Peering is an agreement to interconnect two networks. For example a peering link between Google and the cable company Comcast provides a physical link for streaming YouTube videos, Gmail emails and Google searches of Comcast's fourteen million customers between the company's networks, avoiding any third party Internet provider (Blum 2012).

Network providers and Internet companies get together regularly to bid for and arrange for peer connections. The companies reach service agreements enabling the exchange of data across their different networks. These connections provide scalability and the essential additional pathways for carrying data. They help support the expansion and robustness of the Internet, which would otherwise be restricted to a series of isolated networks and not be the interconnected worldwide web we benefit from today (Blum, 2012).

Data centres

The data that runs across the Internet is stored in huge data centres, run by companies such as Amazon, Google, Facebook and IBM. The best way to visualise data centres is to think of huge warehouses with rows and rows of machines piled on racks. Some of these data warehouses are the size of small towns. So-called 'cloud computing' makes use of these data warehouses to provide a network of remote servers hosted on the Internet to store, manage and process data, rather than using a local server or a personal computer. So, when you hear people talk about 'cloud services' , such as Amazon cloud, what lies behind this cloud is one or more of these buildings, hosting thousands of machines.

Data warehouses may connect to each other for redundancy and failover, meaning that your data is not stored on just one machine. Additionally, virtualisation technology enables one physical machine to host multiple virtual systems, providing a level of abstraction between applications and the underlying physical hardware to support them.

So, if you are using a service such as Adobe Communications Suite cloud version, or Google Apps, the actual application is hosted on a virtual machine in some remote data centre.

History of networks and the Internet

The Internet lacks a central founding figure. Leonard Klinrock is considered by some as the father of the Internet. In 1961 he published the first paper on packet switching, introducing the idea that data could be transmitted efficiently in small chunks rather than a continuous stream, one of the key notions behind the Internet. The first machine providing connection between networks, called an interface messaging processor (IMP) was installed at the University of California in 1969.

The foundations of the Internet go back to the ARPANET project, funded by the US Department of Defence's Advanced research Agency (ARPA) with the aim of developing a network to survive nuclear war. The challenge was to design a network of networks, to enable 'internetworking'. At the start ARPANET linked only four universities, but gradually spread to other universities, military bases, law firms and banks. By 1973 ARPANET had gone international, with a satellite link to University College, London.

By the 1980s the big computer companies, IBM, XEROX and organisations like NASA, were running their own independent networks. A few European networks had also emerged, including EUnet and EARN. But these networks were not connected. In 1983 ARPANET adopted the Transmission Control/Internet Protocol (TCP/IP), which remains the basic building block of the Internet and ensured the standardisation of the Internet's distributed structure. Each independent network is able to communicate with each other using the TCP/IP protocol.

The Internet expanded during the 1980s and included 159,000 computers by the end of that decade. Companies began to establish their own long-distance backbones or network highways. By the 1990s these networks were being connected with the new technology of fibre-optics. However, few organisations had websites. This changed with the advent of web browsers, in particular Mosaic, Netscape and Internet Explorer, which provided an easy means for users to connect to remote computers and enabled the Internet to go mainstream. By 2011 there were 2 billion Internet users and over 35,000 networks (Blum, 2012).

Network models

The Open Systems Interconnection (OSI) model provides a theoretical model for visualising how the Internet was originally designed to work. Although it has been largely superseded by TCP/IP in the Internet, this model still provides a useful framework for understanding what is happening when computers exchange data over a network. This model is a good place to start if you want to understand the technical construction of the Internet.

The Open Systems Interconnection (OSI) Model provides a theoretical model for visualising how the Internet was originally designed to work

Table 1. Open System Interconnection (OSI) Model

#	Layer	Function	Protocols
7	Application	High-level APIs (application programming interfaces), including resource sharing, remote file access, directory services and virtual terminals	HTTP, FTP, SMTP, SSH, TELNET
6	Presentation	Translating data between a networking service and an application, including character encoding, data compression and encryption/decryption	HTML, CSS, GIF
5	Session	Managing communication sessions, that is, continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes	RPC, PAP, SSL, SQL
4	Segments	Reliable transmission of data segments between points on a network	TCP, UDP
3	Network	Structuring and managing a multi-node network, including addressing, routing and traffic control	IPv4, IPv6, IPsec, ICMP AppleTalk
2	Data link	Reliable transmission of data frames between two nodes connected by a physical layer	PPP, IEEE, L2TP, MAC
1	Physical	Specifying the physical cables connecting devices	DSL, USB, ISDN

Routers are the basic post-offices of the network, receiving data packets and sending them to their destination

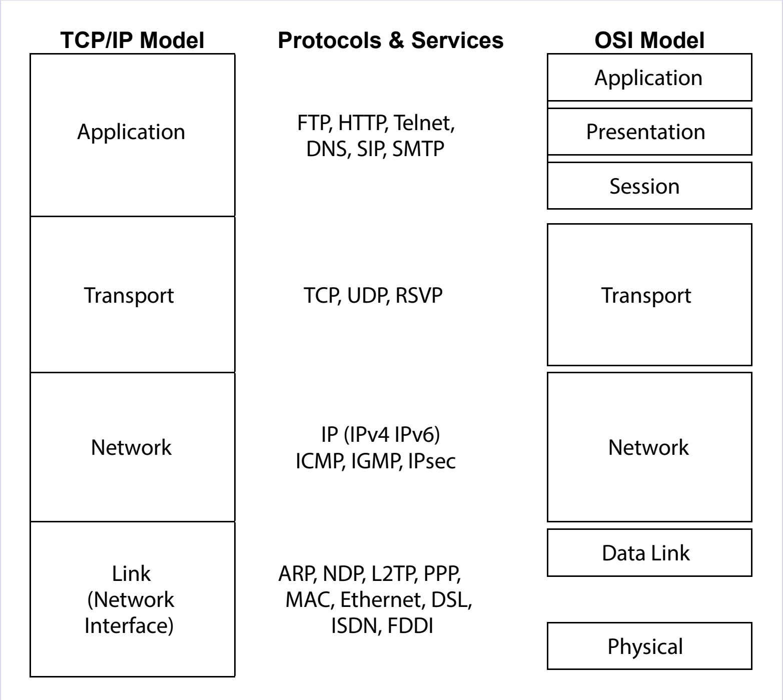
There are seven layers in the OSI model, as shown in *Table 1*. Each layer communicates with the layer above and beneath it. Protocols are the standards that enable data to be sent between computers on a network and processed. At each level of communication, a different set of protocols is supported. So, for example, there are protocols that define the physical cables that connect to your computer and others which define how the data is segmented and then sent across the Internet. There is then a set of protocols defining the session between two computers that are connected and another set defining how the data is provided to applications running on each computer. Finally, a further set of protocols provide specifications for how this data is displayed.

Figure 1 shows the relationship between OSI and TCP/IP models.

Network components

A typical network consists of components designed to handle network traffic. The ethernet cable that plugs in to the back of your office computer is connected to a *hub* or a *switch*. Typically several computers will connect into a switch and form part of a subnet.

Computer traffic from several subnets is transferred to a *router (see Figure 2).* A router operates at the network level of the OSI and TCP/IP models. Think of routers as working like post offices: they receive your data packets, look at the address on the data envelope, and then send it off to the next router, which repeats the process to route your packet to its destination. If you are working from home, your computer will connect to a router, often wirelessly, which then connects to the Internet via the network of your Internet service provider (ISP). Your ISP will then connect to one of the internet exchanges described earlier.



TCP/IP Model	Protocols & Services	OSI Model
Application	FTP, HTTP, Telnet, DNS, SIP, SMTP	Application Presentation Session
Transport	TCP, UDP, RSVP	Transport
Network	IP (IPv4 IPv6) ICMP, IGMP, IPsec	Network
Link (Network Interface)	ARP, NDP, L2TP, PPP, MAC, Ethernet, DSL, ISDN, FDDI	Data Link Physical

Figure 1. TCP/IP model

Acting like regional head post offices, ISP routers are configured to determine the best path for sending your data. The data is then transferred in packets across high-speed cables, often passing through several routers on the way before it reaches the remote computer destination where it is reassembled. Say, for example, you are attempting to retrieve a website page. The remote web server will receive your request, establish a session and present data to your computer, which then displays it on-screen.

In *Figure 2* computers and printers are grouped into two subnets via switches and connected to a router. The router connects to a separate DMZ (demilitarised zone), where public-facing servers are located. The local area network (LAN) router connects to an internet router for access to the Internet.

Types of networks

There are three main types of networks. A LAN connects computers within the same geographical location. Your company office will typically have a LAN. Wide area networks (WANs) connect two or more LANs in separate geographical locations. For example, your company's network may connect different branch office LANs into a central hub. Metropolitan area networks connect two or more WANs in separate geographical locations.

If you want to learn more about core networking concepts, a good book to read is Gibson's *Microsoft Windows Networking Essentials.*

Future of networks and the Internet

What are some of the exciting technologies that are revolutionising the way in which networks and the Internet of the future will be delivered?

The Internet Society is a public organisation that promotes the Internet and has a white paper describing the future of the Internet and scenarios for its development over the next decade.

Privacy and data protection

While technology enables greater connectivity at faster speeds, the debate arises as to how individuals can protect themselves and how societies can legislate to cope with these advances.

With increased connectivity, there are growing concerns over privacy and data security. Cybercrime is one of the fastest growing areas of crime. While the public is concerned with revelations of data hacking and snooping by government organisations, governments are concerned with gaining further abilities to control and monitor the Internet.

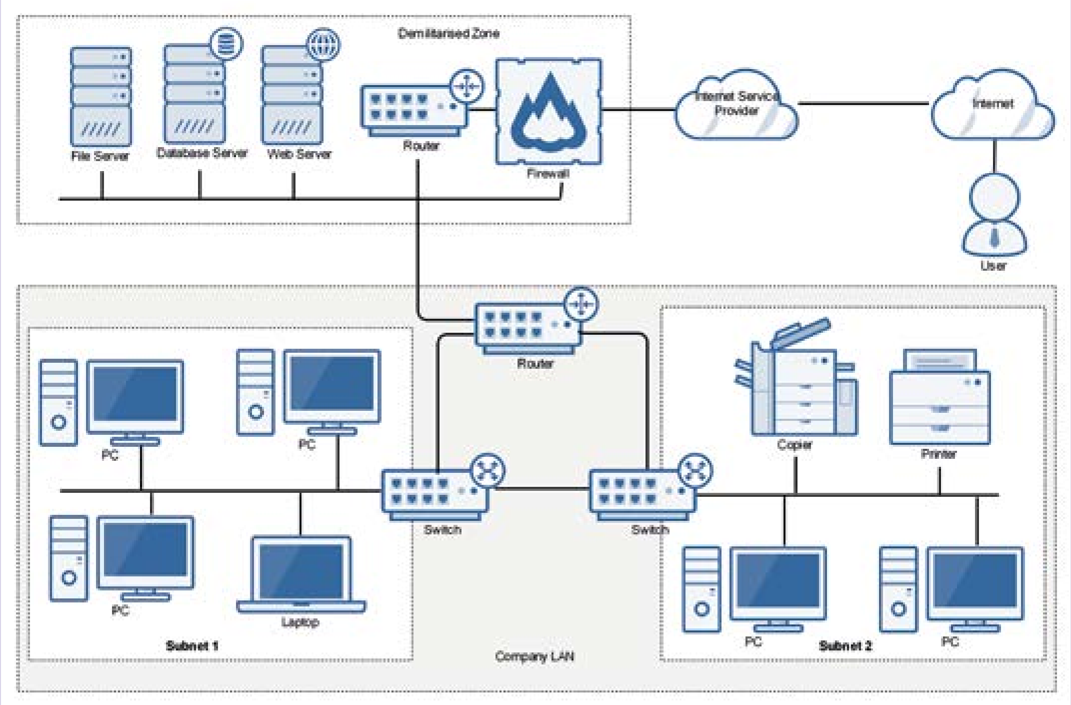


Figure 2. Example of a typical office LAN

For example, the growth of the 'Dark Web' enables encrypted traffic to be passed between browsers, and is typically associated with criminal and illegal activity. To participate in the Dark Web, users install software that encrypts and makes their connection anonymous. The best known system that does this is the 'onion router' Tor, which encrypts data when it is sent and then bounces it through multiple points in the network until it arrives at its destination — each node only decrypting just enough to know where to bounce the message next — hence, only the receiving user gets the actual content.

The Dark Web can be distinguished from the 'Deep Web', which consists of websites, social media profiles, databases, privately shared media (pictures, videos and music) and anything else online that you cannot get to via a search engine, (that is, you need to know the URLs and have the permissions to access them). Some estimate that 99% of content stored on the Internet is part of the Deep Web.

Social media sites, such as Facebook and Twitter, present a challenge for authorities trying to monitor extremism and radicalisation. Firstly, both the media sites and the authorities are reliant on users reporting offensive online material. Secondly, for police or security services to gain access to private material posted by users on these sites, requires special court orders.

The ongoing debate about the balance between individual privacy and safeguarding the public will continue to rage in the years to come, and will influence the future direction of the Internet, as detailed in the Internet Society report.

Expansion of the Internet into our homes

The reach of the network is expanding. British entrepreneur Kevin Ashton coined the term "the Internet of things" to describe how networks of physical objects or 'things' embedded with electronics, software and sensors are increasingly able to collect and exchange data. Consumer devices are becoming smarter and more network-integrated. Household appliances, such as your fridge, stove and room lighting, are increasingly being connected to the Internet, enabling access from a smart phone or other mobile device. Even the clothes we wear are becoming intelligent, for example, wearable technology enables users to monitor their vital life signs and transmit this data to a hospital.

New technology

The basic infrastructure and hardware of the network is also seeing technological advances. Faster routers and new data transmission technology, such as ultra-fast optical networks, will provide faster Internet speeds. The ARPA sponsored Consortium on Wideband All-Optical Networks is developing architectures, technology components, and applications for ultrafast 100 Gbps time-division multiplexing (TDM) optical networks. These TDM networks allow for multiple streams of data to be sent and received at the same time, and on the same channel.

Increasing resilience and interconnectivity

The Internet is becoming more resilient and now interconnects with other types of networks. For example, the 4G standard for mobile telecommunications brings the Internet

The Internet is becoming more resilient and now interconnects with other types of networks

With increased connectivity, there are growing concerns over privacy and data security.

Table 2. Acronyms and terms used in this article

Acronym/term	Description
4G	Fourth Generation. Standard for mobile telecommunications.
AppleTalk	Set of networking protocols developed for Apple Macintosh computers.
ARPA	Advanced Research Projects Agency. Run by the US department of defence.
Bandwidth	Bandwidth is the amount of data that can be transmitted in a fixed amount of time.
CSS	Cascading Style Sheets. Used to define style, layout and behaviour of website pages and applications.
DMZ	Demilitarised zone. This is a separate sub-network containing public-facing servers.
DNS	Domain Name System. A system for naming computers and network services that is organised into a hierarchy of domains.
DSL	Digital Subscriber Line. A protocol used to transmit digital data over telephone lines.
Ethernet	Link layer protocol. Describes how networked devices can format data for transmission to other network devices on the same network segment.
FDDI	Fibre Distributed Data Interface. A set of standards for data transmission on fibre optic lines in LAN.
FTP	File Transfer Protocol. Protocol used to transfer computer files from one host to another host over a TCP-based network.
Gbps	Gigabits per second.
GIF	Graphics Interchange Format. Bitmap image format which is popular on the World Wide Web.
HTML	HyperText Markup Language. The standard markup language used to create web pages.
HTTP	Hypertext Transfer Protocol. The application protocol for distributed, collaborative, hypermedia information systems, which is used for data communication on the World Wide Web.
ICMP	Internet Control Message Protocol. Used by network devices such as routers to send error messages.
IEEE	Institute of Electrical and Electronics Engineers.
IGMP	Internet Group Management Protocol. This is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships.
IMP	Interface Messaging Processor. The first-generation of packet-switching routers.
IPsec	Protocol suite for secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.
IPv4	The fourth version of the Internet Protocol (IP), which uses 32-bit IP addresses (e.g. 192.0.2.235).
IPv6	The latest version of the Internet Protocol (IP), which uses 128-bit IP addresses, represented as eight groups of four hexadecimal digits (for example, 2001:0db8:0000:0042:0000:8a2e:0370:7334).
ISDN	Integrated Services for Digital Network. A set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network.
ISP	Internet Service Provider. Responsible for connecting users to the Internet.
LAN	Local Area Network. Connects multiple computers and subnets together to form a network.
L2TP	Layer 2 Tunnelling Protocol. Used by an ISP to enable the operation of a virtual private network (VPN) over the Internet.
MAC	Media Access Control address. Also called a physical address, is a unique identifier assigned to network interfaces for communications on the physical network segment.
MAN	Metropolitan Area Network. It is similar to a WAN but spans an entire city or campus.
Mbps	Megabits per second.
NDP	Neighbour Discovery Protocol. Part of the Internet Protocol suite used with IPv6.
OSI	Open Systems Interconnection. A reference model for how applications can communicate over a network.
PAP	Password Authentication Protocol. An authentication protocol used by PPP to validate users before allowing them access to server resources.
PPP	Point-to-Point Protocol. A data link protocol used to establish a direct connection between two nodes.
RPC	Remote Procedure Call. Protocol used by one program to request a service from a program located in another computer in a network
RSVP	Resource Reservation Protocol. Used to reserve resources across a network for an integrated services Internet.
Scalability	Scalability is the capability of a system, network, or process to handle a growing amount of work, or its potential to be enlarged in order to accommodate that growth.
SIP	Session Initiation Protocol. A standard protocol for initiating an interactive user session.
SMTP	Simple Mail Transfer Protocol. Internet standard for email transmission.
SQL	Structured Query Language. Used for managing data held in a relational database management system (RDBMS).
SSH	Secure Shell. A cryptographic (encrypted) network protocol used to allow remote login and other network services to operate securely over an unsecured network.
SSL	Secure Sockets Layer. The standard security technology for establishing an encrypted link between a web server and a browser.
TCP	Transmission Control Protocol. The core protocol of the Internet protocol suite, providing reliable, ordered, and error-checked delivery of a data stream between applications running on hosts communicating over an IP network.
TDM	Time-division Multiplexing. A method of transmitting and receiving independent signals over a common signal path.
TELNET	Protocol used on the Internet or LAN to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection.
UDP	User Datagram Protocol. A transport layer protocol defined for use with the IP network layer protocol.
URL	Uniform Resource Locator. A reference (an address) to a resource on the Internet.
USB	Universal Serial Bus. Protocol that defines the cables, connectors and communications protocols used in a bus for connection, communication, and power supply between computers and electronic device.
WAN	Wide Area Network. Connects two or more LANs.

to mobile devices and enables access to areas which lack physical cables.

Satellite technology is opening up the Internet to new geographical regions. Google and SpaceX are reportedly working on a $15 billion plan to develop a new low-orbit satellite network consisting of hundreds of small satellites, which will provide Internet access to remote areas lacking mobile or cable. Further projects to provide Internet access to hard to reach areas include another Google-backed idea to use solar powered balloons floating above commercial air traffic, and not to be outdone, Facebook plans to launch Internet-broadcasting drones the size of Boeing 737s.

Finally, new high-speed cables are being laid under the oceans. A cable from Portugal to Brazil, will transfer data between continents in 0.2 seconds, bypassing the current main link between Europe and the US.

Relevance to technical communicators

Whatever your role or industry you work in as a technical communicator, networks will be relevant to you. You will at some stage in your career need to either understand, use or document aspects relating to network technology.

We live and work in an interconnected world and our ability to use technology and communicate is based on the networking infrastructure, which underpins it all.

In conclusion, networks such as the Internet may not be a magical way of transporting data from anywhere to anywhere else, but they are technological marvels that form the lifeblood of our high-tech society and are central to how we work as technical communicators.

References and further reading

4G Standard: https://en.wikipedia.org/wiki/4G (accessed November 2015)

Blum, A. (2012) *Tubes, a Journey to the Center of the Internet*, 1st Edition, New York, HarperCollins

Curtis S (2015) Google 'to invest in $1bn SpaceX internet satellite programme' www.telegraph.co.uk/technology/google/11357291/Google-to-invest-in-SpaceX-internet-satellite-programme.html (accessed November 2015)

Gibson, D. (2011) *Microsoft Windows Networking Essentials*, Indianapolis, Wiley Publishing Inc.

Internet of things: https://en.wikipedia.org/wiki/Internet_of_Things (accessed November 2015)

Internet Society: www.internetsociety.org (accessed November 2015)

Low Orbital satellite networks: http://arstechnica.com/information-technology/2014/06/google-to-deploy-180-low-orbit-satellites-that-provide-internet-access (accessed November 2015)

OSI Model: https://en.wikipedia.org/wiki/OSI_model (accessed November 2015)

Patterson T and Crane R (2015) http://edition.cnn.com/2015/10/30/tech/pioneers-google-facebook-spacex-oneweb-satellite-drone-balloon-internet (accessed November 2015)

Selected Areas in Communications, IEEE Journal on Issue 5 • Date June 1996 http://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=10916

Submarine link from Europe to Brazil: http://optics.org/news/6/7/4 (accessed November 2015) TCP/IP Model: www.omnisecu.com/tcpip/tcpip-model.php (accessed November 2015)

Ultrafast broadband: www.btplc.com/News/Articles/ShowArticle.cfm?ArticleID=1F647C20-6F61-4E0F-A545-E23443E128AB (accessed November 2015)

Warren Singer MISTC is a founding partner of Cambridge Technical Communicators, based in Cambridge, UK. He has 20 years' international experience as a technical communicator.
E:warrens@technical-communicators.com
W: www.technical-communicators.com

Wael Elazab MISTC is a technical editor with roots in journalism. He works with science, technology and engineering content for print, digital and social media.
E: waelelazab@gmail.com
T: @waelae