Bring Your Own Device FOR SCHOOLS

An introduction to the technologies and terminology

POCKET GUIDE

Future Classroom Lab
by European Schoolnet

European Schoolnet

Contents

BYOD Pocket Guide: an introduction to the technologies and terminology

This is one of four shorter 'pocket guides' that has been developed from the full report, Bring Your Own Device for Schools: Technical advice for school leaders and IT administrators that was published by European Schoolnet with support from Acer and the GSMA as part of the work of Ministries of Education in its Interactive Classroom Working Group (ICWG). It is designed for school leaders or new IT Administrators in schools that have decided to implement a Bring Your Own Device strategy and who are looking for practical, introductory advice regarding the technical aspects of doing this. The publication may also prove useful to more experienced IT Administrators who are interested in other schools' experiences of BYOD implementations.

This pocket guide includes explanations of some basic concepts, common terms and acronyms. It is intended to help non-technical school leaders and staff when discussing BYOD and especially network requirements. Having some grasp of basic concepts and terms is important to enable informed discussions of the key technical issues that will need to be addressed when planning BYOD.

Related pocket guides that you may find helpful:

- "BYOD Pocket Guide: Technical Advice for School Leaders and IT Administrators". - This pocket guide is an abridged version of the full BYOD Technical Guidelines: Bring Your Own Device for Schools: Technical advice for school leaders and IT administrators.
- "Cloud computing and BYOD" - Using cloud based services in addition to BYOD increases the extent to which students can be both location and device independent.
- "BYOD Technical risks planning" - Planning for the introduction of BYOD should include a risk planning process. This guide describes some of the risks, their impact and how they might be prevented or mitigated.

Broadband

ADSL, VDSL, SDSL and SHDSL broadband connections

ADSL (Asymmetric Digital Subscriber Line) is the cheapest type of broadband connection as it uses ordinary copper phone lines rather than requiring any special line to be installed. Theoretically, ADSL can provide up to 24 Mbps download speed with much slower upload speed. However, both speeds depend upon the condition of the wires, the distance to the provider's location and the amount of interference on the line so the speeds actually achieved can be very significantly less than the theoretical maximum.

VDSL (Very high bitrate Digital Subscriber Line) makes more efficient use of the copper phone lines and, therefore, can be up to five times faster for downloads and ten times faster for uploads compared with ADSL. Again, the suppliers' promised up-to speeds are based on ideal conditions and actual speeds achieved are likely to be lower.

SDSL (Symmetric Subscriber Digital Subscriber Line) is generally considered to be a legacy technology and has been succeeded by **SHDSL (Symmetrical high-speed digital subscriber line).** These are similar to ADSL but offer equal download and upload speeds. This can be an advantage to users, which are usually businesses or organisations rather than households, that need to upload significant amounts of video and other bandwidth hungry content. They also have the advantage of separation of upload and download streams so that downloading is not slowed down by other users uploading and vice versa. Unlike ADSL ,telephone traffic cannot share the same wires as data on SDL or SHDSL.

Fibre Optic broadband – Super-fast, Ultra-fast, FTTC, FTTP, etc.

The fastest broadband connections are provided using fibre optic cable, that is sometimes referred to as Super-fast or Ultra-fast Broadband. The term **Super-fast Broadband** is frequently used by companies marketing broadband services but it often just means broadband products that provide a maximum download speed greater than 24 Mbps, i.e. faster than ADSL connections.

The price of a broadband connection usually depends upon the speed of downloading data, for example when a supplier promises a speed of 30 Mbps they usually mean the maximum download speed delivered will be 30 Mbps. The speed at which data can be uploaded is usually substantially less, especially for domestic customers, as it is assumed that they will want to upload data infrequently.

Theoretically **Ultra-fast Broadband (UFB)** has the potential to deliver up to 1 Gbps for both uploads and downloads but services offering lower download speeds, and considerably lower upload speeds, are more commonly offered by ISPs (see **Data Transfer Rates** for an explanation of Gbps and Mbps).

Some suppliers now guarantee minimum speeds as well as promising potential maximum, or "*up to*" speeds for fibre connections. Some also offer services in which speeds are capped to offer a lower guaranteed minimum speed for a lower price.

Where your school connects to the fibre optic cable has a significant impact on the speed of the connection you receive. A variety of four letter acronyms starting with the letters FTT are used to describe these connections, the two most common being FTTP and FTTC.

FTTP - Fibre to the Premises - is a pure fibre-optic cable connection running from an Internet Service Provider (ISP) directly to the user's address.

FTTC- Fibre to the Cabinet – is much more common and cheaper than FTTP and combines traditional copper wire cable and fibre optic cable. The expensive to install fibre optic cable runs to a street metal cabinet which contain telecommunications equipment and then more economical copper wire is used to connect schools (and homes and businesses) to the cabinet.

FTTP provides the fastest connections, much faster connections than FTTC, but is much more expensive both to the supplier and the end users and many providers only offer FTTP connections to businesses. However, FTTC does deliver very good fast connections.

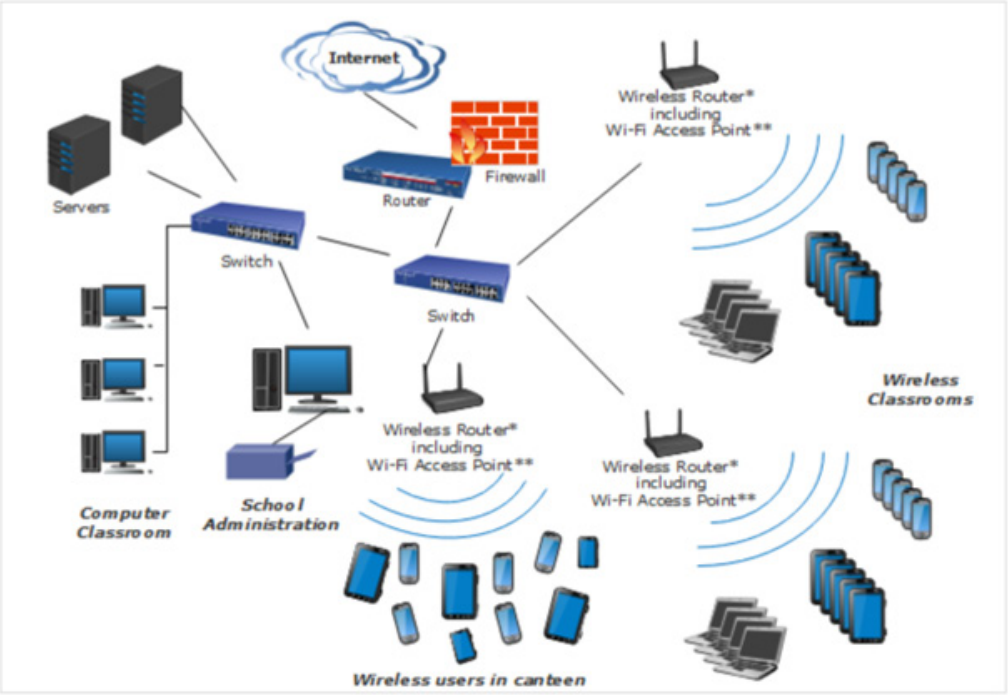
Symmetrical Cable Broadband

Modern organisations, including educational establishments, are increasingly finding that modern methods of working and learning mean they are using their broadband connections for uploading data more than they used to. Voice over IP (VoIP e.g. Skype) services, online collaboration tools, social media services (e.g. YouTube) and cloud computing all involve uploading as well as downloading data. Therefore, broadband services offering only limited capacity for this will increasingly seem inadequate.

A potential solution currently being developed is **Symmetrical cable broadband**, providing speeds of 5 to 10 Gbps for both downloading and uploading and sometimes referred to as **Full Duplex**. CableLabs a not-for-profit consortium responsible for the telecommunications standard used to provide fibre optic Internet access via a cable modem (Data Over Cable Service Interface Specification or DOCSIS) have forecast[1] that the first Full Duplex trials will take place in 2017.

1 http://www.lightreading.com/cable/cable-business-services/cablelabs-first-full-duplex-trials-in-1-year/d/d-id/728774

School network example



*Wireless routers are usually controlled by a WLAN controller that may be integrated, a separate device or cloud based ** Wi-Fi Access Points are typically integrated into routers but may be separate devices

Local area network (LAN)

A local area network (LAN) is a group of computers and associated devices e.g. printers that share common, traditionally wired, communications links to a server, or servers, and a broadband service. LANs operate in a limited area, typically a building or group of buildings e.g. a school (see school network example diagram) and can be linked to other LANs to form a Wide Area Network (WAN).

Wireless local-area network (WLAN)

A wireless local area network (WLAN) is a computer network that may be standalone or part of a LAN and links devices using a wireless method within a limited area such as a school, home or office building. This gives users the ability to move around within a local coverage area and yet still be connected to the network which usually includes a connection to the Internet.

Network name or SSID

An SSID, or Service Set Identifier, is sometimes referred to as a **network name** and is a unique up to 32 alphanumeric character identifier attached to the header of packets data sent over a WLAN. The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID.

School network structure

The structure of school networks varies considerably dependent upon many factors including how recently it was first installed, the size of school, the nature of the building or buildings, the extent to which computers and mobile devices are used, how much cloud computing is used, etc., etc. Figure 6 provides an example of some of typical devices that may be part of a school network and how these may be connected.

Routers, hubs, switches, wireless access points and controllers

Some network managers and technicians tend to use the terms router, hub, switch and access point interchangeably, which can be rather confusing, and further confusion can arise as two or more of these technologies may be combined into a single device. These technologies are also sometimes referred to as edge devices, an **Edge device** being a device that provides an entry point into the core network of an organisation or service provider.

Routers, in computing, are networking devices that forward data packets between computer networks. They are located at gateways where two or more networks connect. For example, where your school's local area network (LAN) and your internet service provider (ISP)'s network connect or where your wired LAN connects to your WLAN. Routers read headers attached to data packets and look up forwarding tables to determine the best path for forwarding data.

A wireless router is a device that performs the functions of a standard network router and also includes the functionality of a wireless access point (see below). For most people the most familiar type of wireless router is one in their home that passes data between personal wireless devices and the Internet.

Hubs are common connection points for all devices in a network. The weakness of simple hubs is that when they receive data they broadcast it to all devices on the network and not just to the one that requires it. This creates unnecessary traffic on the network and impacts network performance.

Switches also forward data packets to devices but they keep a record of the addresses of all the devices connected to them and can therefore send the data directly to just the specific device that needs it. Switches also handle sharing of bandwidth between devices more efficiently than hubs which also helps with network performance.

A wireless access point (sometimes called a transceiver) is a piece of networking hardware that allows Wi-Fi compliant devices to connect to a wired network (and via this to the Internet) by receiving and transmitting data. The access point may connect to a router (via a wired network) as a standalone device or it may be a component of a router. Standalone wireless access points are sometimes referred to as **"autonomous" or "fat" access points**[1] and are less common nowadays. A **"thin" access point** is one that is managed by a WLAN controller.

A WLAN controller provides thin access points with their configuration and also functions as a switch for all the wireless traffic. The use of a controller and "thin" access points is much more scalable than using "fat" access points as this approach saves network administrators the chore of having to manually configure multiple "fat" access points. WLAN controller software, or **virtual WLAN controllers**, can also run on some "thin" access points without the need for a separate, and more expensive, hardware controller. Alternatively, schools can subscribe to a cloud based WLAN controller solution.

A **dual band access point** is one that contains two transmitters, or radios, one operating on the 2.4 MHz frequency band and one operating on the 5MHz frequency band. Dual band access points can be helpful in avoiding interference between access points located near each other. If they are operating on different bands, as well as on different channels within bands, more access points can be installed to support large numbers of users wanting access at the same time in a relatively small area (see frequency bands and channels explanation below).

Cat5/Cat5e/Cat6/Cat6a cables and Crosstalk

The quality of the cables used to connect the wired components of a school's network is important in terms of both the data speeds they can facilitate and how successfully they prevent interference or "crosstalk" between the data they carry. Cat (Category) 5e (Cat

1 http://www.securedgenetworks.com/blog/Controller-vs-Controllerless-Wifi-Whats-the-Difference

5 enhanced) is currently the most commonly used in new networks; it can support 1000 Mbps speeds and 100 MHz bandwidth and is designed to greatly reduce crosstalk. Cat 5 is made to an older standard, supports 10 to 100 Mbps speeds and up to 100 MHz bandwidth, includes less crosstalk protection and is generally considered to be obsolete. Cat 6 can support 10 gigabit data speeds and 250 MHz bandwidth and includes further improvement of crosstalk reduction. However, Cat 6 can only support 10 gigabit data speeds over a cable length of 164 feet. Cat6A cable can maintain 10 Gigabit speeds for 328 feet and exceptionally thick plastic casing helps further reduce crosstalk.

Power over Ethernet (PoE)

Power over Ethernet (PoE) is used to supply electricity to networking, audio visual and computing devices connected to a network without the need for power sockets or adaptors. The power supply and the data are transported along the same cable. However, running power supply through a data cable can cause performance and efficiency issues because it heats up the cable. Therefore the category of cable used for PoE is important. An article on the website of the networking and cabling company Belden[2] suggests that, "As much as 20% of the power through the cable can get "lost" in a 24-gauge Category 5e cable, leading to inefficiency" and advise that Cat 6a cables are more efficient and better able to dissipate generated heat. The Irish Government advises[3] schools that "*PoE may require additional or new cabling runs. Where this is the case Cat 6a or a higher rated cable should be used to future proof requirements. Using Cat 6a instead of Cat 5, for example, ensures higher data rates can be supported*".

Wireless signals, Wi-Fi, Radio Frequency, Bandwidth, Bands and Channels

Wireless signals are electromagnetic, or radio, waves travelling through the air. These waves are extremely useful as they can carry information. Common uses include radio, television, mobile phone, satnav, Wi-Fi and Bluetooth signals.

2 "3 Reasons Why Power over Ethernet Demands CAT 6A Cable", Belden, 2016

3 "Guidance document for the provision of wireless network installations in post primary schools" Department of Education and Skills, Ireland (2016)

Radio Frequency (RF) is a measurement representing the rate at which wireless signals vibrate or oscillate. Frequency is measured in Hertz and is the count of how quickly a signal changes every second. Millions of vibrations a second is Megahertz (MHz) and one thousand Megahertz is one Gigahertz. Higher frequencies allow faster transmission of data. This is usually described as having more **bandwidth**. Higher bandwidth allows files to download and upload faster and the performance of streaming video is much smoother and faster.

Wi-Fi means communication using Radio Frequency (RF) rather than through wires, therefore wireless. Strictly speaking Wi-Fi is a registered trademark of The Wi-Fi Alliance, an international consortium of companies which, since 1997, have followed the Institute of Electrical and Electronics Engineers (IEEE) approach to agree on standards called the IEEE 802.11 protocols. These protocols enable interoperability between products using them, including routers, hubs, switches, access points and Wi-Fi enabled ICT devices like laptops, tablets and smartphones.

Wi-Fi signals operate in two different Frequency **Bands**, usually referred to as just Bands, dependent upon the frequencies they use. The 2.4GHz frequency band is most commonly used by Wi-Fi technologies. It has the advantage of being able to pass through walls and windows quite well. However, as so many devices use 2.4GHz the signals can interfere with each other. Wi-Fi technologies using the 5GHz frequency band and can achieve higher data transfer speeds. However, the signal cannot pass through walls and windows as well as the 2.4GHz signal. Therefore the range of 5GHz technologies is often shorter.

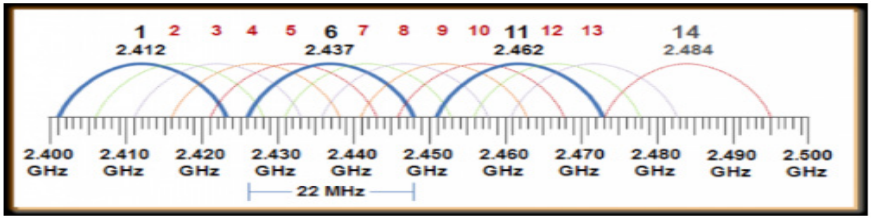
Frequency bands are divided into **channels** and devices located near each other and operating in the same channel can interrupt each other. The website of the Commotion community of contributors[4] (Commotion is a free, open-source communication tool that uses wireless devices to create decentralized wireless networks) includes a useful simile for the problem of interference within frequency band channels. They say "*Each channel is similar to rooms at a party - if one room is crowded it is hard to carry on a conversation. You can move to the next room, but that might get crowded as well*".

This situation is exacerbated in the 2.4 GHz band by the fact that channels also overlap (see diagram). So, although the band includes 14 channels, only channels 1, 6, and 11 are separated from each other by sufficient frequency that they do not overlap. Also some (typically channels 12, 13 and 14) are reserved for specific non-Wi-Fi communication e.g. television and satellite signals.

4 https://commotionwireless.net/docs/cck/networking/learn-wireless-basics/

There are twenty five 20 MHz wide channels in the 5 GHz frequency band and these do not overlap but the use of some of them is restricted with those that can be used for Wi-Fi being dependent upon regulations enforced in each country.

2.4 GHz Channels[5]



The Internet Protocol Suite (TCP/IP),IP addresses, IPv4 and IPv6

Internet Protocol suite (IP suite or TCP/IP) is the conceptual model and set of communications protocols used on the Internet and on most other computer networks. It's common name of TCP/IP is taken from the original protocols in the suite i.e. the Transmission Control Protocol (TCP) and the Internet Protocol (IP), although many more protocols have since been added. IP specifies the format of packets of data and the addressing scheme for computers to communicate over a network. IP is often compared to a postal system in which someone addresses a package and puts it into the system but there is no direct link between them and the intended recipient. TCP/IP establishes a connection between two devices which then send messages back and forth for a period of time.

There are currently two versions of Internet Protocol operating, IPv4 and an upgraded protocol IPv6. IPv4 is the most widely used protocol connecting devices to the Internet and it can provide just over 4 billion device addresses. However as the Internet grows

5 From http://boundless.aerohive.com/experts/WLAN-Channels-Explained.html

unused IPv4 addresses are quickly running out because every device that connects to the Internet requires an address, including computers, tablets, smartphones, game consoles and a rapidly growing number of Internet of Things (IoT) devices.

IPv6, also sometimes called IPng (Internet Protocol next generation) has been designed to provide vastly more addresses. IPv6 also introduces other important improvements to Internet Protocol, including faster data transfer rates and significant security benefits. A large number of Internet Service Providers (ISPs), data centres, cloud services, and software products now support IPv6 and adoption is slowly increasing. However, according to statistics generated by testing by Google[6], worldwide adoption of IPv6 grew from 10% of internet users at the end of 2016 to approximately 16.5% in July 2017.

Network Port

A network port is a process-specific, or application-specific, software construct which acts as a communication endpoint and is used by protocols within the Internet Protocol Suite concerned with communicating with external processes and devices. Networking processes or devices use a specific network port, or ports, to transmit and receive data. Each port has a unique number which is assigned and recorded by the Internet Assigned Numbers Authority (IANA). Port numbers 0 to 1023 are well-known numbers that are allocated to standard server processes. For the Internet, unencrypted data traffic, identified by the letters HTTP at the beginning of the internet address or URL, uses port 80 and encrypted data traffic (HTTPS) uses port 443. Schools may block traffic using other ports in order to prevent circumvention of their safeguarding controls.

The IEEE 802.11 wireless protocols

The 802.11 wireless standards have been evolving over the years since 1997 with more up-to-date standards supporting enhanced functionality and performance for users of Wi-Fi (see diagram).

6 https://www.google.com/intl/en/ipv6/statistics.html

The IEEE 802.11 wireless protocols[7]

Wireless Transmission 802.11 Protocols					
Standards	**Year Established**	**Band Frequency**	**Maximum Data Transfer**	**Channel Bandwidth**	**Antenna Configuration**
802.11a	1999	5 GHz	54 Mbps	20 MHz	1 x1 SISO
802.11b	1999	2.4 GHz	11 Mbps	20 MHz	1 x1 SISO
802.11g	2003	2.4 GHz	54 Mbps	20 MHz	1 x1 SISO
802.11n	2009	2.4 & 5 GHz	600 Mbps	20 & 40 MHz	Up to 4x4 MIMO
802.11ac	2013	5 GHz	1.3 Gbps	20, 60, 80, 160 MHz	Up to 3x3 SU-MIMO
802.11ac Wave 2	2015	5 GHz	3.47 Gbps	20, 60, 80, 80+80, 160 MHz	Up to 4x4 SU-MIMO & MU-MIMO

Clearly, regardless of the bandwidth of a school's broadband, the speed of connection (the data transfer rate) achievable via the routers, hubs, switches, access points in the school's network is dependent upon the protocol they use.

When discussing improvements to his school's wireless network Dario Zucchini in Italy reported that it had been "*updated from this year with a new, even more powerful AC band system* [i.e. IEEE 802.11ac] *that can potentially handle tens of thousands of users*".

7 From Collier M, 2015, "5 Things You Need to Know About How Your Wireless Network Impacts Your Devices" http://mcollier.blogspot.com.mt/2015/09/5-things-you-need-to-know-about-how.html

Also, if students' and teachers' devices do not support fast protocols they cannot fully benefit from improvements to school broadband and the network. For example many laptops only support 802.11b or g. However it is possible to upgrade laptops' Wi-Fi speed by plugging in an inexpensive 802.11ac Wi-Fi dongle. Tablets and smartphones have been designed to take advantage of more recent and faster protocols.

Data transfer rates

The speed at which data travels along a broadband or Wi-Fi connection is measured in megabits per second (Mbit/s or Mbps) or increasingly in gigabits per second (Gbit/s or Gbps) and in future Terabits per second (Tbit/s or Tbps) is forecast.

SISO, MIMO and MU-MIMO

Early 802.11 standards designated one antenna on a router to transmit and the other single antenna at a device to receive data, this is known as Single Input Single Output (SISO). When multiple devices are using one transmitted signal the speed experienced by each is reduced.

The newer protocols support Multiple Input and Multiple Output (MIMO) i.e. multiple antennae at the transmission point producing multiple streams of data (up to 4) to devices requiring Wi-Fi, thereby increasing performance for each significantly. MU-MIMO (Multi user MIMO) enables up to 8 separate streams.

Network monitoring and management tools

As computer networks have become more complex, with more components supporting more users of more fixed and mobile devices in more locations, network managers have required software tools to assist with the necessary tasks of monitoring and managing them. Swiss law requires that schools use Network Monitoring Tools to keep track of all network connections and to store these for 6 months. Philippe Devaud, an IT Adviser in one of the Switzerland's regional ICT Centres advises schools to subscribe to a cloud based SaaS (software as a service, sometimes called on-demand software) Network Monitoring and Management Tool as these are more cost effective than systems bought to install on school servers.

Security and safeguarding

Firewall

A firewall is a network security system that uses rules to control incoming and outgoing network traffic. It acts as a barrier between a trusted network (e.g. a school's internal network) and an untrusted network (e.g. the Internet) and only traffic that conforms to the definitions in the firewall policy is allowed onto the network with all other traffic being denied. Firewalls can consist of hardware or software or both. A hardware firewall can be purchased as a stand-alone device but they are typically found in broadband routers.

Proxy server

A proxy server also helps to protect a network and its users. It acts as an intermediary between a device and a server from which it is requesting a service. The proxy server may be installed on the same machine as a firewall or may be on a separate server. In

companies and schools a proxy server is used to facilitate security, administrative control or caching services and can speed up response times as frequently requested websites are likely to have been previously stored in the proxy server's cache.

Using a proxy server shields the identity of a device or server it is acting as an intermediary for, as it is the proxy server's IP address that can be seen by others not the IP address of the device or server itself. This is helpful for schools in guarding against hacking. However, because of this, proxy servers can also be used by technically sophisticated students to circumvent restrictions schools have put in place which limit what students' IP addresses can access according to the profile created for them.

Virtual Private Network (VPN)

Organisations, including schools, often use a Virtual Private Network (VPN) to communicate confidentially over a public network, typically the Internet. For companies it is a way of connecting remote workers to corporate systems or branches to global offices. Schools may use VPNs to connect separate buildings to the school network or to facilitate communication between groups of schools sharing IT facilities. A VPN provides a secure, encrypted "tunnel" for information transmitted between the two locations. Individuals may also use VPN services if they wish to protect their online activity and identity. One reason they may do this might be because they are using free Wi-Fi access in a public place and are concerned that this may not be very secure. Individuals also often use VPNs to circumvent security arrangements that prevent them from accessing services they have not paid for or are not authorised to access. In schools this might include social media, games and entertainment websites that the IT Administrator does not permit students to access.

Content/information filtering, blacklists and whitelists

Content or information filtering is the use of a software programme to screen and if necessary, exclude from access or availability web pages or e-mails users of the programme consider objectionable (e.g. pornographic, racist violent or hate-oriented) or a nuisance (e.g. spam emails). In companies and schools content filtering is part of the firewall. In schools filtering software is also often used to prevent access to websites school leaders feel are a distraction or wasteful of school bandwidth e.g. social networking and

computer games websites. Parents can also use filtering software on home computers to screen the content their children have access to.

Filtering software can enable users to set up whitelists or blacklists of websites that can or cannot be accessed. Blacklisting allows individual websites that schools do not want students to access to be blocked. Blacklists grow overtime and, to be useful, need to be managed. Dario Zucchini in Italy advises that many schools use a blacklist compiled and kept up-to-date by the University of Toulouse [8]and download updates of newly blacklisted "adult, phishing and other inappropriate sites" every night. Although, it should be noted that the more technically talented students in secondary schools will probably know how to bypass blacklists. Whitelists is a much more extreme, and rather old fashioned, version of content filtering as this prevents access to all websites except those on the whitelist. However whitelisting is much more difficult and time consuming to manage than blacklisting. It requires initial research to identify all the websites all staff and students are likely to wish to access, which is not a trivial task, and then constant updating as access to more sites is requested.

IT staff could also implement whitelists or blacklists of applications which can or cannot run on school devices used by students. It is also possible to blacklist proxy servers or VPNs or to whitelist only specific IP addresses that are authorised to connect to the school network.

DNS, DNS filtering and Smart DNS

Every website, like all devices that access the Internet, has a unique IP address and the DNS (Domain Name System) associates these addresses with domain names. When an Internet user types a URL containing a domain name into a search engine the DNS is used to look up the IP address of the website associated with that domain name. DNS is described as being like a telephone directory as it finds the website with a specific IP address number using the domain name.

DNS blocking or filtering is a common and simple method of denying access to specific websites by removing the records associating their names and IP address numbers from the DNS. Therefore, when the name is typed into a browser the website cannot be found.

8 https://dsi.ut-capitole.fr/blacklists/index_en.php

However, DNS is a distributed network of databases, so if users, e.g. students, wish to get around DNS filtering they can do so by using another DNS database to look up the website they wish to access. There are many Smart DNS services available on-line which enable their users, including students, to do this.

Traffic/Packet shaping

Traffic shaping, also known as packet shaping, involves regulating network data transfer by delaying the flow of data packets that have been designated as less important or less desired than those of prioritized traffic streams. Regulating flow into a network, i.e. downloading data, may be called **bandwidth throttling** and regulating flow out of a network, i.e. uploading data, is known as **rate limiting**. If a school uses traffic shaping tools they can, for example, define how much bandwidth students can use for YouTube so that this remains available for all users but overuse by individual students will not negatively impact on use by teachers for groups of students in classrooms.

SSL

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that data passed between the web server and browsers is private. SSL is used by millions of websites to protect their online transactions with their customers and customers recognise when it is being used by the padlock symbol, the word Secure and the letters HTTPS appearing by the website's URL i.e:

802.1X wireless protocol, Radius and LDAP servers for access control

IEEE 802.1X is generally more secure than the standard IEEE 802.11 protocols which are well documented and well understood by many people and therefore more vulnerable to abuse. It also provides more secure access control for devices connecting to Wi-Fi services as it includes authentication of devices seeking to access the network rather than simply requiring that the correct access key is provided. With IEEE 802.1X protocol authentication a client device (e.g. laptop, tablet or smartphone and sometimes referred to as a 'supplicant' i.e. device that is asking for something) that wishes to attach to the network provides credentials (user name and password or digital certificate) to a wireless access point which forwards these credentials to an authentication server (also known as a RADIUS server) for verification. This verification usually involves consulting a database (often via an LDAP - Lightweight Directory Access Protocol - server). If the authentication server determines the credentials are valid, the wireless access point allows the client device access. This process is sometimes described as similar to a visa check at immigration control at an airport before a traveller is allowed to enter a country. Under Swiss law school systems must include RADIUS/LDAP authentication. Antonio Santos in Portugal agrees "***it is essential to have a centralized authentication (OpenLDAP) and Network access control (Radius + 802.1x)"*** to ensure only approved users can get in the school network.

WEP, WPA and WPA2

WEP, WPA and WPA2 are encryption algorithms used to secure the information passing along a wireless connection. WEP (Wired Equivalent Privacy) was the original encryption algorithm used by IEEE 802.11 wireless networks and is still used in many domestic and some small business Wi-Fi implementations.

However, many years ago a flaw was discovered in WEP which meant it could be cracked relatively easily by people with the necessary knowledge and an ordinary laptop. Therefore, an improved approach, WPA (Wi-Fi Protected Access) was developed. Once again an issue was discovered that meant WPA was not as secure as had been hoped and WPA2 was the solution developed. There are two types of WPA2 implementation, Pre-Shared Key (PSK) Mode for home Wi-Fi networks and WPA2-Enterprise for companies and other organisations wanting government-grade wireless security. IT Administrators usually configure 802.1X authentication to work with WPA or WPA2-Enterprise encryption.

Acronyms

3G	3rd Generation
4G	4th Generation
ADSL	Asymmetric Digital Subscriber Line
AP	Access Point
BYOD	Bring Your Own Device
BYOT	Bring Your Own Technology
Cat5	Category 5
Cat6	Category 6
CCC	Co-Channel Contention
CCI	Co-Channel Interference
DNS	Domain Name System
FTTC	Fibre To The Cabinet
FTTP	Fibre To The Premises
Gb	Gigabyte
Gbps	Gigabits Per Second
GHz	Gigahertz
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol - Secure
IANA	Internet Assigned Numbers Authority
IEEE	Institute Of Electrical And Electronics Engineers
IP	Internet Protocol
IPng	Internet Protocol Next Generation
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISP	Internet Service Provider
LDAP	Lightweight Directory Access Protocol
LAN	Local Area Network
MAMS	Mobile Application ManagementSystem
Mbps	Megabits Per Second
MDMS	Mobile Device Management System
MHz	Megahertz
MIMO	Multiple Input And Multiple Output
MU-MIMO	Multi User MIMO
OTA	Over The Air Distribution
PoE	Power Over Ethernet
PSK	Pre-Shared Key
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role Based Access Control
RF	Radio Frequency
SaaS	Software As A Service
SISO	Single Input Single Output
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
Tbps	Terabits Per Second
UFB	Ultra-Fast Broadband
URL	Uniform Resource Locator
VDSL	Very High Bitrate Digital Subscriber Line
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WYOD	Wear Your Own Device

Glossaries of technical terms

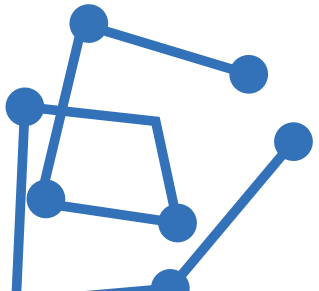
The following on-line glossaries provide explanations of technical terms and are kept up-to-date

Webopedia (www.webopedia.com) say their definitions come from "standards bodies, technology companies, universities, professional online technical publications, white papers and professionals working in the field" and are never based on just one source.

Watis.com (http://whatis.techtarget.com) describes itself as "a reference and self-education tool about information technology. The site provides readers with definitions and fast references. It is updated daily and used by IT and business professionals. Site content is researched and written by editorial and content editors assisted by technical experts from over 60 countries".

Gartner IT Glossary (www.gartner.com/it-glossary) is described as a "trusted guide to exploring technology terms and definitions, from the world's leading IT research and advisory company".

Techopedia (www.techopedia.com/dictionary) provide tech jargon definitions, articles and tutorials for "IT professionals, technology decision-makers and anyone else who is proud to be called a geek".



Future
Classroom Lab
by European Schoolnet

Bring Your Own Device for Schools

Pocket Guide: An introduction to the technologies and terminology

This is one of four shorter 'pocket guides' that has been developed from the full report, Bring Your Own Device for Schools: Technical advice for school leaders and IT administrators that was published by European Schoolnet with support from Acer and the GSMA as part of the work of Ministries of Education in its Interactive Classroom Working Group (ICWG). It is designed for school leaders or new IT Administrators in schools that have decided to implement a Bring Your Own Device strategy and who are looking for practical, introductory advice regarding the technical aspects of doing this. The publication may also prove useful to more experienced IT Administrators who are interested in other schools' experiences of BYOD implementations.

BMB Bundesministerium für Bildung
direção-geral da educação
DZS Ölm zahraničí spolupráce
HITSA Information Technology Foundation for Education
INDIRE Istituto Nazionale Documentazione Innovazione Ricerca Educativa
educa.ch
Le Gouvernement du Grand-Duché de Luxembourg Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse
PDST Professional Development Service for Teachers
T.C. Milli Eğitim Bakanlığı
The Norwegian Centre for ICT in Education
acer
GSMA

http://fcl.eun.org/icwg

futureclassroomlab europeanschoolnet #FCL_eu