Table of Contents

Appendix 1: Internet Standards

Most protocols used by computers and network technology now follow a standard framework known in short as the OSI Model, invented in the 1970's. Further overview of the model can be found at https://en.wikipedia.org/wiki/OSI_model

The use of standardized protocols means that equipment from different manufacturers will inter-operate. It is this standardization that made the Internet possible. Human nature being what it is, there is always someone re-inventing the wheel, along with people and companies seeing an advantage in having a unique product they can monetize. So not all Internet protocols fit the OSI model and not all products are completely interoperable. As electronics and computers advance technically, they are getting smaller and much more complex and unfortunately less interoperable.

Internet Protocol

Internet Standards are created and published by the Internet engineering Task Force (IETF) . Internet Standards create interoperability of systems on the Internet by defining protocols, message formats, data schemas and display and data handling languages. The most fundamental of the Internet Standards are the ones defining the Internet Protocol. This family of protocol standards are commonly known as TCP/IP after the 2 protocols that form the basic functional layers historically. Increasingly, all the complexity of the Internet is completely hidden from our view or knowledge. One last vestige of that is the http that precedes all browser addressing, though increasingly that is not actually displayed by programs.

IP Address Space Exhaustion

The main address space of the Internet, maintained by IANA, was exhausted on 3 February 2011, when the last five address blocks were allocated. Since 1983, when IP address allocation started, the 4.29 Billion addresses in IP V4 have now been used up. The increasing acceleration of Internet technology adoption was recognized in the 1990's and a new address scheme, called IP V6, was published in 1998. IP V6 has a much larger address range but is not compatible with IP V4. Adoption of IP V6 has been very slow, with nearly all tech products still using an IP V4 technique called Network Address Translation to bypass the restrictions of the lack of addresses. NAT allocates addresses at a single location with non-routable address blocks that are translated into legal addresses for communication across the Internet. Since IP V6 is not interoperable with the older address scheme, this global issue will take a long time to resolve.

IPV4 Network Address Translation

A home or enterprise network will normally put all its devices on one of three "private" Internet Protocol (IP) address ranges. These are 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255 and. 192.1680.0 – 192.168.255.255. Consumer products for addresses at home usually use the 192.168.0 address range. Commercial and Government network products most often use 10.0.0.0 address ranges in North America.

Since many thousands of network locations are all configured with non- unique addresses, the Internet Service Providers allocate real IP addresses to their clients as needed by active devices that are then used in NAT functions in the router onsite in your modem.

You can find your current IP address at http://whatismyip.host/; however, you need to be aware that this may change periodically.

Ethernet MAC Addressing

Each device designed and manufactured to be used on an Ethernet Local Area Network uses not an IP address but a unique Media Access Control (MAC) address. Until very recently this was a unique number etched into the chip structure of the communications chip in the device. This address cannot be routed over a wide area Network such as the Internet, but has been used to identify devices for authentication and licensing purposes for nearly 50 years. The MAC address is most frequently used in the cell phone networks to create the cross-connection with the telephone systems numbering scheme and the IP addressing allocation if a data connection is required. Unfortunately, the programmed ability to mask the MAC address has now become an avenue for malicious threat attacks that has created vulnerability.

Virtual MAC addresses are now being used in many applications to mask the true identity of the device,similar to the NAT technique to allow routing for private IP addresses. While this was a good idea to protect consumers from infiltration, it also allows the threat agents to remain hidden, so this direction may create more problems than the one it was intended to solve.

Encryption

Modern Browsers are nearly all built to refuse to open websites that are not encrypted as a defence against malware attacks on Internet users. This makes it essentially mandatory now to run an encrypted web site.

Encryption is implemented on the Internet using Public Key Infrastructure (PKI) which uses a protocol called SSL/TLS and is visible in the web site address starter label, 'https'. A certificate is a file that mathematically shows browsers or other software that they've made an encrypted connection to the site they attempted to connect to.

To enable HTTPS on your website, organizations , or their agents, obtain a certificate (a type of file) from a Certificate Authority (CA). There are many thousands of CA's, not all of them useful, inexpensive or safe to use. A recommended free CA is https://letsencrypt.org/ which can guide you in this process. Note that the domain registration information for DNS of your site will also be needed. If you have paid for a website developer to build your website and it is hosted somewhere on the Internet, it is common for the host site company to also offer DNS and PKI Certificate services.

Annual Fees amount to $20 to $50 a year per domain host name used, so encryption, while essential, is not a major expense in your IT budget. Subscription cycles are available from 1, 2 or up to 10 years. It is very important to renew the certificate and DNS entries with the Domain and Certificate authorities.

If your library is hosted by the BC Libraries Cooperative, this is all looked after in your contracted service with them.

Local Area Networks

The data network in your library is based on a group of network standards known as Ethernet. Developed at Xerox PARC in USA in the 1970's, the basic Ethernet network technology is called Carrier Sense Multiple Access with Collision Detect (CSMA/CD) and is IEEE Standard 802.3, approved in 1983. There are nowadays many extensions and modifications to the original standard to allow higher speeds, many more workstations and different media such as copper cable, fibre optics and radio.

Power Over Ethernet

PoE is a technology that delivers power to the WIFI access point (and other devices) over the data cable from the data switch, so avoiding the installation of 110v AC power outlets specifically to power the WIFI. The PoE standard is an IEEE 802.3af Ethernet network standard development upgraded in 2012 and 2018 to now include power up to 100 Watts. The latter has not yet been approved by the Building Codes administrators in Canada. It is very important to use the highest standard data cable in your network installation projects in order to support the delivery of PoE and future proof the infrastructure for higher speeds as they are introduced.

WIFI

There are 2 standard organizations regulating the WIFI radio systems in Canada.

The actual radio regulations are the responsibility of the Canadian Government, found on the Internet at
https://www.canada.ca/en/health-canada/services/health-risks-safety/radiation/everyday-things-emit-radiation/wi-fi.html

The technical specifications for the equipment sold for WIFI service are produced by the IEEE and are found at 802.11 standards. WIFI is a trademark owned by the Wi-Fi Alliance, a USA industry group dedicated to certifying that WIFI products meet the standards. The names of the products were rebranded recently from the IEEE's 802.11 series to WIFI 4, 5 and, new in 2019, WIFI 6.

Radio networks can be tricky to design and install in library buildings because the signals can be blocked by building walls, columns, floors and ceilings and bookshelves. Use a dealer with network discovery and testing capability (often an application on a cell phone nowadays) to design and purchase your WIFI capacity. You are not delivering a home network for convenience so when buying WIFI equipment, remote management integrated with your data network and the ability to run through Power over Ethernet (PoE) are both important functions that should be on your list of requirements. This mostly rules out home consumer products. New commercial Wireless Access Points (WAP's) are customizable with different aerials and mounting points , wireless mesh networks and are usually powered by PoE. These features allow you to place the devices to the best coverage points in your building with the fewest number of cables.

New WIFI equipment using WIFI5 standards should offer at least two radio bands, a 2.4GHz band and a 5GHz band. The 2.4GHz band offers better range because it is more adept at penetrating walls and other structures. However, it doesn't offer the throughput and lower latency that you get with the 5GHz band radio. Three separate networks are often defined on these 2 bandwidths, (2 networks are defined on the 5GHz band) segregating the different patron groups from staff requirements perhaps. The latest Wi-Fi protocol, 802.11ax, is also known as Wi-Fi 6 or High Efficiency (HE) Wireless. Wi-Fi 6 is designed to increase throughput to 9.6Gbps with less network congestion, greater client capacity and better range performance using improved wireless technologies. This could include Orthogonal Frequency-Division Multiple Access (OFDMA) and Target Wake Time (TWT). OFDMA improves overall throughput by breaking Wi-Fi channels into sub-channels, allowing up to 30 users to share a channel at the same time.

Target Wake Time (TWT) is designed to reduce power consumption, extending battery life for mobile devices such as phones and tablets as well as devices such as security cameras and video doorbells that are often battery powered for home installation.

No sooner will WIFI 6 be available in 2021 than another is on the horizon. WIFI 6E operates on a new 6-7 gHz radio band and is not certified for use in Canada as of 2020. It may be at least 3 to 5 years before product is available in Canada.

Cabling Standards

Data cabling systems for customer premises are guided by standards to create very structured systems that support many possible uses and media.

1. In Canada and USA, the standard is ANSI/TIA-568-C, also known as the Commercial Building Telecommunications Cabling Standard. The ANSI/TIA-568-C standard is a specification adopted by ANSI (American National Standards Institute in 1991.
2. The International Standard on Information Technology Generic Cabling for Customer Premises is the ISO/IEC 11801 Ed. 2 standard.

These documents are very similar.

The cabling standard breaks structured cabling into six areas:

1. Horizontal cabling
2. Backbone cabling
3. Work area
4. Telecommunications rooms and enclosures
5. Equipment rooms
6. Entrance facility (building entrance)

The cabling should be installed by certified cabling technicians. The certifying authority in Canada and USA is BISCI, the Building Industry Consulting Service International organization.

Network management information of all the Internet Services that a library can subscribe to is deployed by and considered confidential by the ISP's. That management information is not shared with customers even during issue resolution events.

You can of course manage the LAN interface to the ISP 'modem' device with a management tool of your own, if only to be able to determine if the ISP service is actually working as sold. This is highly recommended, when your only support is a 1-800 number. Bear in mind that if you have an IP phone service, this will be a cell phone call you need to make if you have no landline phone.

Network Management

The network management services in a Local Area Network are based on a protocol named SNMP (Simple Network Management Protocol). In 2004, the IETF recognized SNMPV3 as defined in RFC3411-3418 as the current standard and it is not a full Internet Standard. The new standard is an attempt to improve the security of the SNMP protocols and processes through use of encrypted channels and processes.

Security issues have been extremely common for as long as SNMP has been deployed. Version 1 is still the only widely deployed level but is known to have serious security weaknesses. Version 3 is now widely deployed in new IT purchases but may require complex encryption support from IT staffs and care needs to be taken to introduce these tools with a new management system vendor.

<---Back to Main Index   NEXT Appendix 2 - vendor links--->