Notes for: IDS 3917-U01C (54121) VIP Pgm-B (Directed Individual Study)

In a very simplistic explanation Computer Networks are created as follows:

We have multiple sciences that come together to create Computer Networks.
- Computer Scientists develop the software that is needed.
- Computer Engineers, Electrical Engineers, Mechanical Engineers and Material Engineers, among others, create the hardware.
- Information Technology Professionals Merge and mantain the Software and hardware together to create Computer Networks.

Many of the names/technologies used in this class are Engineering concepts that fall out of our knowledge area, so we will not go into detail of the meaning of their meanings, I will simply explain what do they do, but not how.

WHAT IS A COMPUTER NETWORK.
===========================

A Computer Network consists of a group of multiple hardwares and softwares to solve a specific problem.

We have many types Servers found in Computer Networks such as:
- Data Processing
- DNS
- Web
- Fax
- Email and many more (as learned in our Operating System for IT class)

Usually a Computer Network is made out of multiple types of Computer Networks, as describe above, working together.

NETWORK TOPOLOGIES
==================

Networks have a physical and a logical part.
The physical side of the Networks are the foundation of our overall system.
It relates directly to the wiring.

Some physical sides covered in this class are: the bus, the token ring, star, mesh and the hybrid.

The logical layout of the networks relates to the method of accessing the network, the parts that you can not see or touch, the flow of information and other data.

PHYSICAL SIDE

BUS, all connects all nodes to single pipeline also called backbone.
All signals get on, travel to the destination, and get off the backbone.
Main problem, if the backbone gets damaged all connectivity is lost. Similar to current Xmas trees, on elight bulb gets disconnected and then all other light bulbs turn off.

TOKEN RING

Similar to bus topologies but can have redundancy, usually in setups that use Fiber Distributed Data interface (FDDI) https://www.google.com/search?q=TOKEN+RING&rlz=1C1CHBF_enUS783US783&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjxlfuVhZviAhWNMd8KHTHfCs0Q_AUIDygC&biw=1455&bih=717

STAR

There is a center (a hub, switch, router) to where all connections/nodes are connectected.
if one node gets disconnected the rest of the network continues working.
If the hub fails all connects fail

https://www.google.com/search?rlz=1C1CHBF_enUS783US783&biw=1455&bih=717&tbm=isch&sa=1&ei=FrfaXNjSMeSm_QbiqayoAQ&q=star+topology&oq=STAR+&gs_l=img.1.2.0i67l4j0j0i67l3j0j0i67.29920.36649..39902...0.0..0.107.1059.13j1......2....1..gws-wiz-img.....0..35i39.YrRt6A9B8sc

MESH

Where all connections are conected to each other. Very expensive and complex to build, but very reliable because of its redundance and resistance to outages.
The internet is a large mesh used in mission critical services

https://www.google.com/search?rlz=1C1CHBF_enUS783US783&biw=1455&bih=717&tbm=isch&sa=1&ei=FrfaXNjSMeSm_QbiqayoAQ&q=mesh+topology&oq=MESH&gs_l=img.1.0.0i67j0j0i67j0l7.2473.5996..8857...0.0..0.217.1284.11j1j1......2....1..gws-wiz-img.....0..35i39.VzuudnaWS5Q

HYBRID

Hybrid systems are create by combining multiple topoligies such as stars, ring, wireless connected to bus selecting the best of each for specific needs.

https://www.google.com/search?rlz=1C1CHBF_enUS783US783&biw=1455&bih=717&tbm=isch&sa=1&ei=drfaXOrZIq-AtgX38ruwBQ&q=hybrid+topology&oq=HYBRID&gs_l=img.1.0.0i67j0j0i67l2j0l4j0i67l2.37309.39150..41945...0.0..2.98.1161.13......2....1j2..gws-wiz-img.....0.xi0CrqUz344

Today, rouge wireless access points, a smartphone, and/or a little social engineering can LOGICALLY put a hacker into a system without actually obtaining physical access.

A Computer Network consist of the following

CABLES

1) Cat Cables 1-7 (NOT ETHERNET CABLES, ETHERNET IS A PROTOCOL)
   The Different Types of Cat Cables
   Mbps = megabits per second = One milion bits per second
   UTP = Unshielded Twisted Pair
   STP = Shielded Twisted Pair
   SSTP = Screened Shielded Twisted Pair

   The basic difference between UTP and STP is UTP (Unshielded twisted pair) is a cable with wires that are twisted together to reduce noise and crosstalk. On the contrary, STP (Shielded twisted pair) is a twisted pair cable confined in foil or mesh shield that guards the cable against electromagnetic interference.

   SSTP (Screened Shielded Twisted Pair) CAT6 cables. Category 6a Cable. Category 6a (CAT6a), also known as Augmented Category 6, requires a cable to operate at a minimum of 500Mhz and provide up to 10 Gigabits of bandwidth.

Cable Type	Maximum Data Transmission Speed	Max Bandwidth	
Category 1	1 Mbps		tel land lines
Category 2	4 Mbps		tel land lines
Category 3	UTP 10 Mbps	16 MHz	
Category 5	UTP 10/100 Mbps	100 MHz	
Category 5 e	UTP 1,000 Mbps	100 MHz	

Category 6	UTP or STP	1,000 Mbps	250 MHz	
Category 6 a	SSTP	10,000 Mbps	500 MHz	
Category 7	SSTP	10,000 Mbps	600 MHz	
Category 8		40 Gbps	2000 MHz	backward CAT 6A compatible

Cat 1 - 7 Maximum length 100 meters (~330 rounded up feet (328.084 feet))
Cat 8 Maximum length 30 meters is fully backward compatible with Category 6A

https://www.google.com/search?rlz=1C1CHBF_enUS783US783&biw=1455&bih=717&tbm=isch&sa=1&ei=obfaXMGDDYT0tAX2p6b4Dw&q=NETWORKING+CABLES&oq=NETWORKING+CABLES&gs_l=img.3..0l5j0i5i30j0i8i30j0i24l3.21469.32427..32872...9.0..1.101.2912.39j1......2....1..gws-wiz-img.....0..0i67j35i39j0i10j0i10i24.J3a5yeCFwY8

http://ciscorouterswitch.over-blog.com/article-the-different-types-of-ethernet-cables-125299851.html

With each successive category, there has been an increase in data transmission speed and bandwidth.

To fully future-proof a network installation, the highest categories are recommended, but only if all of the other equipment on the network is capable of similar speeds. Otherwise, expensive cables will be only as fast as the slowest piece of hardware on the network producing a bottleneck.

A Botleneck can exist at any location in a network, a Cat 1 can become the bottleneck. The network will operate at the slowest speed of any Network part.

Can we create a Network using Cat 1 cables?
Yes but it will be the slowest part of the Network creating a Bottleneck.

Cat cables, from Cat 3 up, have 4 twisted pair sets of cables inside.

Each pair have different colors (usually) green, light blue, red and brown

One cable is solid and the other is striped, example a solid red and a strip white, red cable.

2) Fiber Optics Cables
- Material glass
- Data Transmitted using light
- Speed: The speed of light

  The speed of light in a vacuum is 186,282 miles per second, and in theory nothing can travel faster than light.

  Using the speed of light we could go around the Earth 7.5 times in one second.

  https://www.google.com/search?rlz=1C1CHBF_enUS783US783&biw=1455&bih=717&tbm=isch&sa=1&ei=N7jaXKuuNI6q_QaqtoSQDQ&q=Fiber+Optics+Cables&oq=Fiber+Optics+Cables&gs_l=img.3..0j0i24.84238.84238..89862...0.0..0.77.77.1......1....2j1..gws-wiz-img.QzcyRbWGqhI

3) Coaxil Cables

This type of cable is mainly used today in our homes to get the Non-Fiber Optical connections from the outside of the home into the home for internet service from ATT, Comcast, Direct TV, etc.

https://www.google.com/search?rlz=1C1CHBF_enUS783US783&biw=1455&bih=717&tbm=isch&sa=1&ei=krjaXLG-HM69ggeM77OACg&q=Coaxil+Cables&oq=Coaxil+Cables&gs_l=img.3..0i10i24.172926.172926..176992...0.0..0.71.71.1......1....2j1..gws-wiz-img.9ktqrjy7RLs

4) PVC vs Plenum Cable vs Pipes.

CAT cables have an external flexible case made of PVC or Plenum material. The PVC material is fire flamable and very toxic. When PVC CAT cable is used we need to use it inside a metal or regular PVC pipe. Plenum calbe is also fire flamable, but it is allowed to be installed without being inside a pipe.

https://www.google.com/search?rlz=1C1CHBF_enUS783US783&biw=1455&bih=717&tbm=isch&sa=1&ei=RLnaXKzdE4ru_QbO6KiIDQ&q=PVC+vs+Plenum+Cable&oq=PVC+vs+Plenum+Cable&gs_l=img.3..0i24.34342.37328..38634...0.0..0.167.1066.12j1......2....1j2..gws-wiz-img.....0..0i8i10i30j0i10i24j35i39j0i30j0i8i30j0i5i10i30j0i5i30j0j0i67.MbVtNeHRfIE

CAT Cable Connectors
----

a) RJ45 Connectors are regulary used for Computer Networks.
They have 8 (eight) connectors where the 8 (eight) cables from the CAT cables go in.
Male RJ45 connectors are used for the CAT cables.
Female RJ45 connectors are found inside computers, wall plates, RJ45 female female gender changers, other peripherals   and are used to insert the Male RJ45 connectors.

https://www.google.com/search?rlz=1C1CHBF_enUS783US783&ei=CeHZXLObLY-6ggff14_YDg&q=rj45+connector&oq=rj45+&gs_l=psy-ab.1.2.35i39l2j0l4j0i67j0l3.6798.7707..11039...0.0..0.131.563.4j2......0....1..gws-wiz.......0i71j0i20i263.Akz6WvGmbcY

b) RJ11, RJ14, RJ25 Connectors are regulary used for Telephone Land Lines, used in telephones, faxes and other peripherals.
They have 8 (eight) connectors where the 8 (eight) cables from the CAT 1 cables go in.
Male RJ11, RJ14, RJ25 connectors are used for the CAT 1 cables.
Female RJ11, RJ14, RJ25 connectors are found inside computers, wall plates, RJ11, RJ14, RJ25 female female gender changers.

https://www.google.com/search?rlz=1C1CHBF_enUS783US783&ei=s-HZXOXNDc2c_QbcnKKYDQ&q=rj11+connector&oq=rj11+connector&gs_l=psy-ab.1.0.35i39j0i7i30l2j0j0i7i30l2j0i67j0i7i30j0l2.54429679.54431221..54438629...0.0..0.90.332.4......0....1..gws-wiz.......0i71.LjOAnaC0T-A

c) Gender Changers
Sometimes we have peripherals that need to get connected together, and they have the save type of connections, either male male or female female. We have peripherals that are called gender changers which allows us to connect peripherals in cases as this.

https://www.google.com/search?rlz=1C1CHBF_enUS783US783&ei=WbbaXI3RL8GQggfJko_ICg&q=rj11+gender+changer&oq=rj11+GENDER&gs_l=psy-ab.1.0.0i22i30.44468.48142..50993...0.0..0.104.1252.14j1......0....1..gws-wiz.......0i71j35i39j0j0i67j0i20i263j0i131.Qtk6NkcmERM

d) Different Voltage Connectors with Same Configurations
We have cases where the connectors look exactly the same but transmit different voltage. The DB25 connectors are an example. We find DB25 connectors used in serial communications (one bit at the time) and also DB25 connectors used in parallel comunications (eigth bits at the time). The parallel transmitions require a larger amount of voltage and if we connect a parallel connector into a serial connector, the serial peripheral accepting the larger voltage will very likely get damaged.

https://www.google.com/search?rlz=1C1CHBF_enUS783US783&biw=1455&bih=717&tbm=isch&sa=1&ei=a7naXKaaLebI_QaG4YaABg&q=DB25+connectors&oq=DB25+connectors&gs_l=img.3..0i24.86579.86579..88815...0.0..0.76.76.1......1....2j1..gws-wiz-img.JzzeO8Q7TNE

It is very important that we understand our cables, connectors and voltages.

TCP/IP Protocol

TCP/IP is the protocol that we use today in most Networks and Internet connectivity

CAT Cables Used in TCP/IP Connections

CAT cables have 4 pairs twisted cables making them 8 cables. In TCP/IP communications, that uses CAT cables, a total of 4 cables are needed, therefore each CAT cable has 4 spare cables, or we can create 2 full TCP/IP connections for each CAT cable.

https://www.google.com/search?rlz=1C1CHBF_enUS783US783&biw=1455&bih=717&tbm=isch&sa=1&ei=xbnaXIHQFYud_Qb6qKqIDA&q=cat+cables+types&oq=cat+cables&gs_l=img.1.2.0l6j0i5i30j0i8i30l3.64635.70810..74495...0.0..1.85.1777.24......2....2j1..gws-wiz-img.....0..0i30j35i39j0i67.Lt3yr6sKjeA

Land Line Telephone Cables Used in Connections

CAT cables have 4 pairs twisted cables making them 8 cables. In Land Line Telephone communications that uses CAT cables, we only need 2 (two) cables per connection, therefore each CAT cable can have 6 spare cables, or we can 4 full connections per cable.

I always recommend that regardless of the connection, always use cat 5 (at least) CAT cables, so that we can use them for multiple hardware connections. The greater cost of cabling an organization is in the labor not in the cable cost.

We can used CAT 1 - CAT 6 cables to create Land Line Telephone connections.

Next week, we will make these types of cables when we cover: Land Line 66 Block (Punchdown Patch Panel).

===

Making CAT 5e Cables
----

https://www.google.com/search?rlz=1C1CHBF_enUS783US783&biw=1455&bih=717&tbm=isch&sa=1&ei=ELraXPb6MYPitQX73L14&q=Making+CAT+5e+Cables&oq=Making+CAT+5e+Cables&gs_l=img.3..0i24.187366.187366..188631...0.0..0.89.89.1......1....2j1..gws-wiz-img.HuMJ_12_kQ8

Today we will provide every student with a 1,000 feet box of CAT 5e cable, and all the necessary tools to make, test, and connect to a live network, the cables that will be made in class.

From the box of cable, each student will cut a 6 feet long cable, will be given 2 RJ45 connectors, wire cutters, PUNCHER?, and a tester to test the cable.

Each student will be instructed on how to make the 6 feet CAT cable, with oversite during the entire process.

Once each cable is made, it will be visually checked and physically tested using a wire tester, then it will be physically tested in the Hardware lab using a live network, where we will take the names of the students whose cable work correctly, to be graded. Students who do not succeed at this time will be given lab time, on front of tutor to learn how to finish this task.

===

Blue Boxes
==========

Also known as Boxes & Brackets are used for low voltate cabling management, These boxes allow to secure the cables inside the wall, to which we well install the wall plates that will hold the connectors where we punch down the cables.

https://www.homedepot.com/p/Carlon-1-Gang-Non-Metallic-Low-Voltage-Old-Work-Bracket-SC100RR/100160916?MERCH=REC-_-SearchPLPHorizontal1_rr-_-NA-_-100160916-_-N

Wall Plates
===========

Wall plates are mostly made of plastic and they are white, beige and other colors.
We place the desired connector (usually female connectors) that will terminate the CAT or other types of cables in the wall plates.

Wall Plates are placed on the Blue Boxes or Brackets shown above.

https://www.google.com/search?q=wall+plates&tbm=isch&tbs=rimg:CRyThsXmbxBqIji0r-Pj7UuNxPd19hKodEqP0JS7hzgRe4yuXNFrMm_1RnXKGoQk91xdI8qVLgNRKS6MZqDfWRJwCqSoSCbSv4-PtS43EEdJtrsdNdpgCKhIJ93X2Eqh0So8RuDLxxlgCNGUqEgnQlLuHOBF7jBGm0ZWIn8dPfioSCa5c0Wsyb9GdEbgZzFeGn5lcKhIJcoahCT3XF0gRsMMacZjNksIqEgnypUuA1EpLoxEGnHx19Cx87SoSCRmoN9ZEnAKpEXUP8hldW_1Nz&tbo=u&sa=X&ved=2ahUKEwia3tWKvZ3iAhVMhuAKHUUCBVoQ9C96BAgBEBs&biw=1455&bih=717&dpr=1.1

Punchdown Patch Panel
=====================

We have many different type of Punchdown Patch Panels, some are wall mounted, others inside cages, and others on setups.

https://www.google.com/search?q=mounting+a+patch+panel&tbm=isch&tbs=rimg:CcohagkfqR7yIjgJmjBloSrqnuGXv4CxWCKiZr08_1Lwc2uglGMFjcRmQ3COmSJklv5WrzvZmi6ex8vz64ieKY24-eyoSCQmaMGWhKuqeEX7vzsw_1CDcdKhIJ4Ze_1gLFYIqIRz_1_16tgWiF14qEglmvTz8vBza6BHFnQtWGNwP8SoSCSUYwWNxGZDcETX8PRxborAQKhIJI6ZImSW_1lasRxBF0660sQCYqEgnO9maLp7Hy_1BGWQdrHGWwhuyoSCfriJ4pjbj57EbMfzZrhrwsH&tbo=u&sa=X&ved=2ahUKEwi4nP2_wZ3iAhXMc98KHWVZDkAQ9C96BAgBEBs&biw=1455&bih=717&dpr=1.1#imgrc=cheC-biEvMb1rM:

https://www.google.com/search?rlz=1C1CHBF_enUS783US783&biw=1455&bih=717&tbm=isch&sa=1&ei=KP_bXM__BIyJggeSm4mAAw&q=patch+panels+cat+6&oq=patch+panels&gs_l=img.1.1.0l2j0i7i30l8.47388.48829..51903...0.0..0.85.722.10......1....1..gws-wiz-img.RMTrWKHad9A

Land Line 66 Block (Punchdown Patch Panel)
==

These punchdown Patch Panels are used to connect the land line telephone wires provided by your service provider, usually from ATT, going into a building with the new cable runs that we install to bring the service to the user. (faxes, backup phone lines, etc)

https://www.google.com/search?q=land+line+patch+panels&rlz=1C1CHBF_enUS783US783&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjHiKW34IriAhVmUt8KHX5ZAGEQ_AUIDygC&biw=1455&bih=717#imgrc=rfm0Nv7yWku8dM:

Computer Cages
==============

To protect access to Servers, Routers, and other computer equipment we install all computer peripherals and connections inside what is known as Computer Cages.

https://www.google.com/search?q=computer+security+cages&rlz=1C1CHBF_enUS783US783&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjNu9juvp3iAhXNmeAKHWwoBEcQ_AUIDygC&biw=1455&bih=717

Routers
=======

Routers are intelligent peripherals that connect all parts of a network. Routers are programmable to allow and manage access to it from users. Many routers can provide wireless services.

Routers know the mac address of all peripherals connected. MAC addresses are a low level component of an Ethernet network (and some other similar standards, such as WiFi). They allow a device to communicate with a machine on the local physical network (LAN), and cannot be routed across the Internet - because physical hardware might in theory be plugged in anywhere in the world.

IP addresses cover the whole internet, and routers use them to figure out where to send data even if it needs multiple hops to reach its destination - but they aren't helpful in interfacing with the physical hardware on your local network.

https://www.google.com/search?q=computer+routers&rlz=1C1CHBF_enUS783US783&source=lnms&tbm=isch&sa=X&ved=0ahUKEwj4kcSkw53iAhXKnuAKHRSMBB0Q_AUIDygC&biw=1455&bih=717&dpr=1.1

Switches
========

Switches like routers are also programmable to allow and manage access to it from users but it usually has more options than routers.

Switches know the ip address of all peripherals connected. IP addresses cover the entire internet and are also used to connect all networking peripheral.

https://www.google.com/search?q=switches&rlz=1C1CHBF_enUS783US783&oq=Switches&aqs=chrome.0.0l6.4297j0j7&sourceid=chrome&ie=UTF-8

Hubs
====
Hubs are non-intelligent peripherals that can connect all parts of a network. Hubs are sometimes used as repeaters.

Hubs are very slow because they do not know the ip addresses or mac addresses of the connected peripherals so it uses broadcasting, which means it requests the information from all peripherals and then it sends the information also to all peripheral, taking a lot of time and making the system slower.

https://www.google.com/search?rlz=1C1CHBF_enUS783US783&ei=eDHYXP3NCOH45gLF76KwBw&q=computer+networking+hubs&oq=computer+hubs&gs_l=psy-ab.1.3.0l2j0i7i30l4j0j0i30j0i7i10i30j0i5i30.33529.36433..41935...1.0..0.186.828.9j1......0....1..gws-wiz.......0i71j0i10j0i13j0i8i7i30j0i8i13i30j0i8i13i10i30.LoJ223q8rRY

Defaults User Names and Passwords Build-in in Peripherals
===
Routers, Switches, Hubs and many other computing networking peripherals have built-in default user names and passwords. It is very important that when we install a new peripheral we change the user name and passwords. One of the Cyber Security problems we have is that many companies do not change them.

===

Computer Case

Cases are usually made out of Metal and Plastics to encase all the necessary computer parts that make a computer.

Mother Board

Some people say that the computer motherboard is the nervous system of your computer.
A Motherboard is a flat board, usually made of fiberglass, soldering, copper wires, sockets, and many places to connect what we call peripherals/components that will make the correspondind computer, such as workstations, laptops, cellphones, automobile computers, servers, etc.

https://en.wikipedia.org/wiki/Motherboard

BIOS (Basic Input/Output System)

The BIOS (Basic Input/Output System) is a hardware chip found on the motherboard, where we write the software called "The BIOS firmware" which is a set of computer instructions that control input and output operations.

Enables computers to perform certain operations as soon as they are turned on. The principal job of a computer's BIOS is to govern the early stages of the startup process, ensuring that the operating system is correctly loaded into memory.

https://www.google.com/search?rlz=1C1CHBF_enUS783US783&ei=4YfsXL65Gu6e_QbqnqKACg&q=bios+chip&oq=bios+in+computer&gs_l=psy-ab.1.5.0i71l8.0.0..19132...0.0..0.0.0.......0......gws-wiz.oGtW-Sxko4A

CMOS

Hardware chip

CPU

All computers have a Central Processing Unit, also known as CPU.

Currently, the major CPU manufacturers are:
Intel,
AMD.
NVIDIA.
others are:
Qualcomm.
IBM.
Samsung.
Motorola.
Hewlett-Packard, etc

https://www.google.com/search?rlz=1C1CHBF_enUS783US783&ei=9YfsXKzZG7Dp_QatuKto&q=cpu+manufacturers&oq=cpu+manu&gs_l=psy-ab.1.0.0l10.1116883.1125105..1127752...1.0..1.353.2464.0j15j0j1......0....1..gws-wiz.....6..0i71j0i67j35i39j0i20i263j0i131.wl-HqenNkxI

RAM

Random Access Memory (Temporally Memory)

Video Boards

Ports
=====

Input Ports

Keyboard
- USB
- PS/2

https://www.google.com/search?q=keyboard+ports&rlz=1C1CHBF_enUS783US783&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiQuc_worriAhURqlkKHXW1CCAQ_AUIDygC&biw=1455&bih=673

Mouse
- USB
- PS/2

https://www.google.com/search?q=keyboard+ports&rlz=1C1CHBF_enUS783US783&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiQuc_worriAhURqlkKHXW1CCAQ_AUIDygC&biw=1455&bih=673

Video
- Screen Input

https://www.google.com/search?rlz=1C1CHBF_enUS783US783&biw=1455&bih=673&tbm=isch&sa=1&ei=1h7rXM6gAarW5gLdya6gAg&q=video+screen+input&oq=video+screen+input&gs_l=img.3...365156.373117..374412...0.0..0.183.3087.39j1......0....1..gws-wiz-img.....0..35i39j0j0i67j0i10j0i30j0i24.M2hOaVvC480

```
Microphone
https://www.google.com/search?rlz=1C1CHBF_enUS783US783&biw=1455&bih=673&tbm=isch&sa=1&ei=1R3rXMHNCojZ5gLGiYGQAg&q=Microphone+ports&oq=Microphone+ports&gs_l=img.3..0.5246.5246..5916...0.0..0.87.87.1......0....1..gws-wiz-img.uTWdpnwLiRY


Scanner
- USB
- RJ45
https://www.google.com/search?rlz=1C1CHBF_enUS783US783&biw=1455&bih=673&tbm=isch&sa=1&ei=tSPrXJihF6Ty5gLr2IP4Bg&q=Scanner+computer+ports&oq=Scanner+computer+ports&gs_l=img.3...30248.32077..34992...0.0..0.63.510.9......0....1..gws-wiz-img.DtrOYLtTZVQ


Copier
- USB
- RJ45
Today's Business copiers are usually part of Network printers, so they use the same ports that come with the Network Printers


Output Ports
------------
Printer
- USB
- Serial
- Parallel
- RJ45
https://www.google.com/search?rlz=1C1CHBF_enUS783US783&biw=1455&bih=673&tbm=isch&sa=1&ei=0SDrXNr7L6G8gge2r7vABA&q=printer+ports&oq=printer+ports&gs_l=img.3..0j0i5i30j0i24l8.164590.169635..170133...0.0..1.205.2648.33j4j1......0....1..gws-wiz-img.....0..35i39j0i67.aYJcFX2bsPo


Speakers
https://www.google.com/search?rlz=1C1CHBF_enUS783US783&biw=1455&bih=673&tbm=isch&sa=1&ei=fCHrXMW_Ksia_QbAyZ4Y&q=Speakers+ports+&oq=Speakers+ports+&gs_l=img.3...457831.467483..468863...8.0..1.132.1078.15j1......0....2j1..gws-wiz-img.......0j0i30j0i5i30j0i8i30j0i24.kO0Xq8YV2vA

Computer Projectors Ports
- VGA
- VGA to USB
- VGA to HDMI
https://www.google.com/search?rlz=1C1CHBF_enUS783US783&biw=1455&bih=673&tbm=isch&sa=1&ei=syDrXI_OIo2zggfK0o3ABQ&q=computer+projectors+ports&oq=computer+projectors+ports&gs_l=img.3...28125.29098..29338...0.0..0.66.359.6......0....1..gws-wiz-img.......0i24.yDSFpYWRx90



Input/Output Ports
------------------
There are multiple peripherals that can be used as input and output, some are the following:

Video
- USB
- HDMI
- VGA
- DVI
- S-Video
https://www.google.com/search?rlz=1C1CHBF_enUS783US783&biw=1455&bih=673&tbm=isch&sa=1&ei=YBfrXPaRN-nK5gKgr4XwDA&q=video+ports&oq=video+ports&gs_l=img.3..0l5j0i5i30l5.1473095.1477145..1477586...0.0..3.113.1861.23j2......0....1..gws-wiz-img.....0..0i67.CnCcMC_J_Jg

========================================
```

****

The Following pages about the A+ 220-1001 and 220-1002 CompTIA certification are owned by Professor Messer and posted at:

https://www.professormesser.com/

I thank Professor Messer for his great work that benefits all of us

****

Recomendations by Professor Messer:

- DOWNLOAD: CompTIA certification objectives http://CompTIA.org
- Watch Professor Messer videos https://www.professormesser.com/free-a-plus-training/220-1001/220-1000-training-course/
- Get a good A+ book
- Sample exam and questions on Professor Messer website
- Practice Hands-on command line commands
- Watch http://professormesser.com/objectives

0.1 – An Overview of A+ How to Pass Your 220-1001 and 220-1002 CompTIA A+ Exams (13:37)

Topics Covered
hardware
software
netwroking
security
mobile devices

Comptia (Computing Technology Industry Association)

Core 1 and Core 2 exams

What area of computing does A+ 220-1001 cover
Mobile Devices
Networking
Hardware
Virtualization and Cloud Computing
Hardware and Network Troubleshooting

exam is 90 minutes long
Range from 100-900 points
passing grade is 675

What area of computing does A+ 220-1002 cover
Operating Systems
Security
Software Troubleshooting
Operational Procedures

software

Mobile Devices
Networking
Hardware
Virtualization and Cloud Computing
Hardware and Network Troubleshooting

exam is 90 minutes long
Range from 100-900 points
passing grade is 700

What exams do you need to pass to be A+ Certified

Which exam do you need to take first to be A+ Certified

When (how far apart) do you need to take your exams to be A+ Certified

Types of questions asked on the exams
Performance based questions (anything but multiple choice questions)
Multiple Choice questions

When do you know if you pass the exam

When do you know which questions you answered correctly and wrongly

Free monthly study group live streams

1.1 – Laptop Hardware (19:19)

Differences between Desptop and Laptop

Keyboard
keys are next to each other
rigth side grouping page up/down does not exist on laptop (numeric key pad)
Hard disk size 2.5
Solid State no moving parts, silent, faster
Hybrid sshd magnetic and Solid State
Magnetic (Spinning Hard Drive)
Copper cooling heat sink going into a fan

802.11 Wireless card
W-WAN Wireless celullar card
W-PAN Bluetooth card Personal Area Network card

Mini PCI Card for above wireless cards
Mini PCI Express card

Small Outline Dual-in-line memory modules
Micro-Outline Dual-in-line memory modules

RAM chip key purpose

Smart Card Reader purpose - Identification
USB Reader purpose - Identification

CPU processors and video boards are usually built-in into the motherboard so they can not the upgraded

LCD (Liquid Crystal Display) very light and provide very high resolution, very frigile
resolution is fixed to the screen and it can NOT be changed
if you change the resolution via software, the screen becomes blurry

Power supplies are built-in into the computer case
The power conversion is done by an external device that provides DC (Direct Current) power directly into the laptop
The external device can be Auto Switching or direct that convert the AC (Alternative Current) to DC current
The Auto Switching input voltage can be 110 volts or 220 volts
They are very specific to the make and model of the laptop you are using

Lithium Iom (Li-ion) battery

What is the laptop touch pad used for? (mouse)
Pointing stick, that moves in all directions to control the cursor

Where are the speakers in laptop, internal external

CPU, video controller and memory controller, in many laptop CPU are built into the CPU

Laptop CPUs run slower than in desktops because they need to produce as little as possible heat

In laptops Motherboards are built for ONLY one type of CPU

What is the Hard disk size in a laptop

Some of the benefits of Solid State drives are that they do not have moving parts, therefore they are silent and faster.

1.2 - Laptop Displays 220-1001 (7:03)

https://www.professormesser.com/free-a-plus-training/220-1001/laptop-displays-3/

LCD technology

The vast majority of today’s laptops are using LCD technology on the displays. LCD is Liquid Crystal Displays. There’s a backlight that’s on your LCD display that is shining through liquid crystals, color filters, and other components to finally show you the messages and the graphics on your screen.

LCD Advantages

The advantages of using an LCD on a laptop computer are that it is lightweight, which is especially helpful for a mobile device. It’s relatively low power, so we’re going to have as much battery available as possible, and relatively inexpensive, so it keeps down the overall cost of the laptop.

LCD Disadvantages

If your job requires you to match colors or have a very good color representation on the screen, you may find some challenges with LCDs. Because there is a backlight that is shining through, it becomes very difficult to get a true black on the screen. We also have to be concerned about this backlight. If we lose the backlight because of a problem with the LCD or the fluorescent lights that are used to shine through the laptop screen, then suddenly the screen will go black. And then we have to replace the entire screen or different components of the backlight just to have that laptop working again.

OLED (Organic Light Emitting Diode) Technology

One way to get around some of these problems with color representation are to use a different type of laptop display called OLED. It stands for Organic Light Emitting Diode. And OLED is an organic component that lights up when you provide it with an electric current.

OLED Advantages

These are usually very thin and very light screens. It doesn’t require that you have a glass to protect it on the front. And because it’s lighting itself, it doesn’t require a backlight. That means you have very good color representation, especially with true blacks. When there is simply no color, you don’t provide any electric current, and everything stays black.

OLED Disadvantages

Unfortunately, OLEDs are still not very popular on a laptop platform. We have organic materials that tend to degrade over time. And there are problems with decayed images still being displayed on these OLED screens. These OLED displays are also more costly. And they use more of your battery, which are not a great combination for a mobile laptop device.

Antennas Locations

A very important part of your laptop display that you don’t even see are the antennas that are inside the screen. They’re usually multiple antennas. There’s a Wi-Fi main, auxiliary connections, Bluetooth, cellular type connections. And they all wrap around the top of your laptop screen. That’s because when you open your laptop screen, that’s the highest point. So by putting them into and around that laptop screen, we’re able to get them as high in the air as possible.

PCI Express Card

On this laptop, there’s a mini PCI express interface that’s available to install an 802.11 card. You can see the wires are here. And those wires are wrapping around this lower part of the laptop. And they go up into the display itself. And they go up high into the display to be able to get the best signal possible.

Webcams Location

We rely more and more on video communication these days. And so the webcams are being installed onto the laptops themselves. You can find the video capture or real time video transmissions are available with a camera that’s right at the top of the display. These usually have both audio and video capabilities. And you’ll need to make sure you install the correct driver for that hardware, depending on what operating system you’re using.

Microphones

If you look closely, you can see the microphones that are installed at the top of this system. There’s a left and a right microphone. These are useful if you’re on a webcam and you don’t have another microphone available. They’re not high quality. You wouldn’t use this to be able to create online content. But it’s perfect for doing video conferencing.

Here’s a closer shot of this webcam with the audio microphone connections on the left and right side. It’s integrated into the screen itself and doesn’t take any additional space on your laptop.

LCD Backlights

We mentioned earlier that these LCD displays on our laptops have a backlight that is behind the screen. And there are usually two different types of backlights that you’ll find on a laptop. One of these is an LED backlight that’s on the LCD display. Sometimes we refer to these displays as LED displays. And what we’re really saying is that it’s an LCD display that is being backlit with LEDs.

They usually are LEDs that are placed around the edges of the screen. Or it’s making a matrix as you see here and providing the backlight using these LEDs. Because these LEDs are using the same DC voltage that’s available on your laptop, it doesn’t have to do any type of voltage conversion to be able to power these LED backlights.

Most of your newer laptops will be using those LED backlights. But some of your older systems may be using CCFLs. These are Cold Cathode Fluorescent Lamps. These use higher voltage. You need more power to be able to provide that fluorescent backlight. And they’re a little bit thicker than the LEDs.

These backlights are obviously important. We wouldn’t be able to see the screen unless we have a backlight that’s going through the LCD, and finally, we’re able to see it with our eyes. Some laptops will have inverters inside of them that will invert from DC into AC. These are primarily used for those CCFL fluorescent backlights that are in older laptops.

If your LED or CCFL backlights stop working, then the screen will look dark. But if you look very carefully, perhaps use a flashlight, you can still see that there’s information on the screen. It’s just not being lit from your backlight. This means that you’ll need to replace either the inverters on these older laptops, or you may need to replace the entire display to be able to have that backlight working again.

LCD Used as Input Device

Some laptop displays allow you to write directly on the display, because the display itself is a digitizer. You would use a pen-like device, like this stylus, to be able to touch the screen and draw on it as if it was a piece of paper. This is becoming more common on laptops and tablet computers, or in hybrid computers like this one, that have a keyboard that looks very similar to a laptop but has a screen that’s very similar to a tablet. And then I can use this stylus to be able to draw on the screen or use my keyboard both at the same time.

If you prefer not to use a stylus, you could use a laptop screen that has direct touchpad support. So you can touch the screen and input information into that device. These are usually devices that have an option for a keyboard. Or you can use it individually as a single tablet component so that you can input in whichever way makes sense for you.

1.3 - Laptop Features 220-1001 (9:14)

https://www.professormesser.com/free-a-plus-training/220-1001/laptop-features-3/

Laptop Keyboard vs Desktop Keyboard

If you’re used to typing on a full-sized desktop keyboard and then you shift over to a laptop, you’ll notice there’s a lot of keys missing. We don’t have a lot of room on a laptop to be able to put the full set of keys that you might have on a desktop computer.
And so one thing that you’ll notice on this laptop is not only do we have a small area for typing, and then some of the specialized keys like Page Up and Page Down have been moved to the right side– and there’s our arrow keys at the bottom– but you’ll notice there are these blue keys that are also embedded onto the keyboard as well. These are laptop function keys, or Fn keys. You’ll notice there’s a blue Fn button here at the bottom. And by holding down the Fn key, or function key, and then clicking one of these blue buttons, you’ll be able to perform an additional set of features.

Laptop Multiple Video Screens

One very common function key that you would find on many different laptops is one that allows you to control dual displays. Dual displays are referring to both the internal display that’s on the inside of your laptop and then an external display that you can connect to using an HDMI connection or a VGA connection that’s on your laptop.

By using this function key, you can then move between different configurations for video. You might use just the display that’s on the inside of your laptop. You can hit the function display key again and duplicate what you’re seeing on your screen. Maybe you use the function key again and extend this across as if you have two separate displays. And then finally, turn off your laptop display and only project on the external display.

On this laptop, the function key that controls that display is the F4 button. So you would hold down the Function key and then hit the F4. And you can see the blue characters there are referring to the internal LCD display on the laptop and an external display.

Your laptop might also choose which display to use based on whether your screen is open or whether you close it. This is the refrigerator door effect. When you close your laptop screen, you may still be able to use the laptop. But all of your video may output to the external monitor connection. There’s sometimes a physical switch on older laptops. But most of them these days have an internal magnetic switch. So there’s nothing external on the laptop display itself.

The functionality of closing that screen may cause your entire computer to go into a suspend mode. So you have the ability to change whether your computer stays on or whether it turns off, usually in the BIOS or a utility that comes with your laptop.

Wireless vs Physical Network Connectivity

Because these laptops are moving from one place to another, there may be times when you want to use a wireless network and other times where you should not be using a wireless network. Some laptops have a function that allows you to enable or disable this wireless functionality. This might be a physical switch on the side of the laptop like this one here. Or it may be a function key that we would use to be able to enable or disable wireless connectivity.

This may be an all or nothing switch that turns on and off 802.11 Bluetooth and cellular connectivity all at the same time. Or you may have the ability to specify which one of those wireless networks you would like to enable or disable.

Controlling Audio

Another common function key is to be able to control audio. On this laptop, there’s a function key for page up and page down that is also a volume up and volume down. And you’ll notice there’s a function key on the End button that will mute and unmute the audio. This laptop also includes separate buttons for those functions. So you can decrease or increase the audio or mute it, all from these individual, specific buttons on the laptop itself.

Controlling Video Brightness

Most laptops allow you to control how bright your screen might be. So you can control the backlight using function keys. In this case, this laptop has the up and down arrow keys that are also used to increase or decrease that brightness. Of course, you have to keep in mind that if you’re going to increase the brightness, you’re going to be using a bit more power. So if you want to decrease the power, you may be able to conserve a little bit of battery time.

You not only have backlights on your LCD display, many laptops also have backlights on their keyboards. This allows you to see those keys even when you’re in a dark area. You might be able to control the intensity or brightness of that backlight. You might be able to control the duration as well, so when you press a button, how long that particular backlight will stay on. Or you can disable it completely so that it’s not using that light when you don’t need it.

Enabling/Disabling the Touchpad in a Laptop

If you’re using your laptop keyboard and you notice that you’re inadvertently hitting that touchpad and moving the mouse around the screen, there may be a function key that will allow you to disable the touchpad completely. And that way, you’ll never be able to accidentally press a key or move the mouse while you’re using your keyboard.

Video Landscape/Portrait mode

Our modern laptops allow us to use our laptops in different orientations. So we might have it in a landscape mode or a portrait mode, depending on what we’re doing with a particular application. There may be a function key that allows us to switch the orientation. Or there may be a hotkey that’s on the laptop itself that allows us to change what the orientation might be. So we can simply press a button, and it will change from portrait to landscape.

Laptops Specialized Control Buttons

Some laptops might include a number of different media options on the keyboard itself. These are specialized keys that allow us to control the audio and the video that might be playing on our laptop. We can play, stop, rewind, fast forward. There might be mute buttons or volume buttons that we can choose, all by pressing those specialized keys instead of hunting around the screen with your mouse to try to find exactly what section of the screen you should be clicking on.

By using these specialized buttons, we’re able to play, stop, fast forward. We have volume buttons or mute buttons available, all by pressing these specialized keys instead of trying to figure out exactly what function keys or keystrokes would be required.

Laptops GPS (Global Positioning System)

More and more of our mobile devices are including global positioning system, or GPS, capabilities in the device itself. This also is going to use those antennas to listen in to GPS signals. So if you enable or disable airplane mode, you may be enabling or disabling the GPS functionality as well.

Laptops Docking Stations

When you’re traveling with your laptop, you may not need all the functionality of a system that you’re using when you’re inside of your office. But when you come back to your office, you may want to plug into a docking station. This allows you to use an external keyboard and mouse, maybe extend the interfaces on your laptop so they’re always plugged in to printers and other devices that are in your office. You might even have room to have expansion cards plugged into a PCI Express bus that greatly extend the capabilities of your laptop system.

Laptops Port Replicators

Smaller versions of these docking stations may be called port replicators that are simply replicating those interfaces and ports on the back of your laptop so that you don’t have to keep plugging and unplugging different cables when you leave or come back to the office. These port replicators are usually smaller than these larger docking stations, because they usually don’t have those PCI Express interface card options.

Securing your Laptop

Our laptops are very portable. And that’s ideal if we’re planning to travel with this device. Unfortunately, it’s also ideal if somebody wants to walk away with this laptop when you’re not looking. Because of that, you might want to consider using a physical laptop lock.

If you look closely at your laptop, you’ll probably find a small slot that has metal reinforcement. That’s what you use to plug in one of these physical laptop locks. And that will connect it to your laptop. You would then connect the rest of that cable to some other solid object that’s in the area. That way, you could briefly walk away from your laptop and not worry about somebody taking that when you’re not watching.

You can see that these cables are very small and easy to travel with. This one has numbers set for the lock instead of using a key. And there’s a loop on the end so you can connect it to something solid and make sure that nobody’s taking this laptop when you’re not watching.

Hybrid Laptops

An increasing number of our laptops are becoming much more flexible in how we use them. Very often, our laptops have a keyboard and a tablet screen. We can twist them around. We can turn them in different ways.

We can have a presentation from a screen just by spinning the screen around but keeping the keyboard close to us. This allows you to show a presentation on the screen by simply turning the screen around towards the people that need to see that presentation. And you might even have a stylus available so you can draw on the screen as you’re using the presentation mode. Or you might be able to disconnect the screen from the keyboard completely. And then you’re in a tablet mode, and you can use your stylus.

1.4 - Mobile Devices 220-1001 (5:00)

https://www.professormesser.com/free-a-plus-training/220-1001/mobile-devices-2/

Tablet`s Operating Systems

Tablets are one of the most popular categories of mobile devices today. And they’re usually running an operating system such as iOS or Android. They’re usually about seven inches diagonal or larger.

And we’re using touchscreen access on these devices. You can see they don’t have a keyboard. There’s no mouse associated with this. We might also have stylus or other types of input as well, depending on the device itself.

Tablet`s Applications

These tablets can support a wide range of different applications, everything from productivity to games or utilities. And they’re very good at taking pictures or watching movies or other types of media that you might want to use on this tablet device.

Smartphones

Perhaps the most popular mobile device today is the smartphone. This is our mobile communication hub. We can make phone calls. We can text. We can send emails, all from this very small three and 1/2 inch to about six inch diagonal device.

This makes a very good media viewer as well. We can watch movies and watch videos on these devices. And of course if we’re traveling, this is great for getting maps and travel information. And you can run many different kinds of applications on these as well, everything from specialized apps to games and so much more.

Wearable Technology Devices

Wearable technology would be a mobile device that you could wear somewhere on a person. So it might be a smartwatch, for example, which takes the place of the traditional mechanical watches. And usually it integrates with our mobile devices, such as our mobile phones and our tablets.

Another popular wearable device is the fitness monitor, so we’re able to track our heart rate. We can see how much we’ve walked or run today. It’s even able to see how our sleep patterns are working, because it knows when we’re moving and when we’re not moving.

Virtual Reality Devices

With virtual reality devices, we’re completely removing the real world and entering a virtual world. You can see this display that you’d put on doesn’t allow you to see anything that’s outside of that particular screen. With virtual reality, it’s common to use input devices that you would use outside of that display. But all of this input is occurring inside of the virtual world.

This is useful if you’d like to play games. There’s industrial design applications, some applications where you can create art in this virtual world. And because you’re able to move around and look in different places, it enhances the ability to watch videos and to view images, all in this virtual environment.

If you wanted to combine the virtual world and the real world, you would have augmented reality. This is usually accomplished by wearing a special kind of eyeglass. Or perhaps you’re looking through a screen of a tablet or a mobile phone. This would allow you to see things that are in the real world. But the computer would augment or add additional information to the things that you’re seeing through that device.

An example of augmented reality in medicine might be where you’re putting on special glasses and able to see an X-ray that’s superimposed on the patient itself. Or maybe you’re traveling. And as you’re going from place to place, you can see messages pop up on buildings or on roads to tell you where you happen to be. And you might be able to use this in gaming, where part of the real world suddenly becomes part of your game.

e-reader Devices

An e-reader is a mobile device that is specifically created to read books. It might have some capabilities to play music or perform some application use. But most of what you’re doing with an e-reader all revolves around book reading.

Instead of using a color LCD screen, e-readers use a technology called electronic paper. This is a black and white screen that is designed to perform extremely well in direct light. One interesting characteristic of these e-readers is that they have an exceptionally long battery life. When you’re reading information on the screen, you’re not using any of the battery. The only time the battery is used is when you change pages and that information updates on the screen. These e-readers almost exclusively use wireless connectivity. So they may be downloading and updating book information from a Wi-Fi network or a cellular network.

In-Car Navigation GPS Devices

And another category of mobile device is a global positioning system device, a GPS. This is an in-car navigation that gives you turn-by-turn directions on where you need to go. It does require that you have a view of the sky so that it’s able to receive signals from the multiple GPS satellites.

This also requires that you update this information, because our streets and our roads are constantly updated. So usually we’ll have an over the air update that would occur through a wireless network. Or perhaps there’s a memory card that we would install in the GPS to be able to perform this update.

1.5 Mobile Devices Accesories 220-1001

Mobile Devices Connections (6.27)

https://www.professormesser.com/free-a-plus-training/220-1001/mobile-device-connections-2/

Connecting Mobile Devices

There are many different ways to connect to these numerous mobile devices that we use. And there are also many different ways to use our mobile devices to then connect to the internet. In this video, we’ll look at many of these mobile device connections.

One common way to connect our computer to these mobile devices is through a Micro-USB or a mini-USB plug.

These are very standardized especially since the European Union’s standardized that all of the mobile devices in the EU must be able to support this Micro-B plug type connection. If you have an older mobile device, you may find a mini-B plug. You can see, the mini-B plug is a little bit larger than the Micro-B plug.

You’ll also find that newer mobile devices are using USB-C, which is a 24-pin USB connector. And it’s double sided, which means it doesn’t matter which side you plug it in. It’ll work just fine. It’s about the same size as the older USB Micro-B plug. And you can see them next to each other on the screen here.

On the other end of the USB connection is probably a standard USB A connection, just like you always use to connect to your computer. And the USB plug can act as both a USB 2.0 connection or the newer USB 3.1 standard. One nice addition to the USB-C standard is that it can also act as an analog audio output. So there are very inexpensive adapters you can get that will convert from a USB-C connector to a standard analog audio jack.

Connecting Apple Devices

Many Apple mobile devices use a proprietary standard connection called a lightning connector. This is an eight-pin connector. And you’d commonly see this on iPhones and iPads. There are some advantages to using this lightning connector over a Micro-USB connector. One of those is you can output more power through a lightning connector, which means you could possibly recharge your iPhone or your iPad faster than using a traditional Micro-USB connection.

These can also be plugged in either way to your mobile device. There’s no top or bottom. So it doesn’t matter which side you’re plugging it in. It will connect every time. This is also a much simpler design than the older Apple 30-pin connectors that they used to use. And they’re much more durable than those connectors, as well.

Tethering Connectivity

Many of our mobile devices allow us to use tethering to get internet access. We would connect our mobile phone directly to our computer usually over a USB connection. And that would allow us to use the phone as a method to communicate to the internet. So this computer, being directly tied to this phone, would then have the same access to the internet as your phone normally has. This means, if your laptop is not connected to an 802.11 wireless network or it’s not connected to a cellular network using a built-in adapter, you can simply use a USB cable and your telephone to get the access over these cellular networks.

Creating a Wireless Hotspot Using a Cell Phone

Many phones allow you to take this idea of tethering to the next level and turn your phone into an to 802.11 wireless hotspot. This means that any 802.11 device can connect to your phone. And your phone then provides internet access over the cellular frequencies. Both tethering and this wireless hotspot functionality is often controlled by your wireless carrier. So check with your wireless company to see what type of functionality is available on your phone and if there are any costs involved for enabling these capabilities.

In the early days of mobile phones, we had many different cables and connectors that we were using. It seemed that every phone that we used had a different type of connection to be able to power that device. And it was usually a different type of cable if you wanted to connect to that same device and transfer data. Every phone manufacturer had a different way of doing this. And it seemed that they were also changing these connections intentionally with every different model of phone.

European Union Cell Phone Connectivity

The European Union and the market really drove a lot of changes along these lines. And the EU insisted that, if you were going to connect a mobile phone to an external power connection, it must have a standard connector. And the EU standardized on the USB-type connections for every phone that was sold in the EU.

This solved a number of problems for consumers that were having to collect a lot of different cable connections or connect to a lot of different cables to be able to charge their phones. On this single charging system that's on the screen, you'll notice there are multiple cables for Nokia, Nokia, Nokia, and Nokia. Those are four different power types for the different phones made by the same manufacturer. By converting our mobile devices to use one or two different standards for power, we greatly simplified this process for the consumer.

Another type of mobile device connectivity that you might use every day is NFC. Stands for Near Field Communication. This allows you to use your mobile device to transfer small bits of data to other devices. These might be payment systems like the one you see here.

Cell Phones Other Uses

You might be using your phone for transportation. So it can be used as a bus token or a subway token. Or you might want exchange contact information with someone else who might have an NFC-enabled phone. This allows your phone to act as an access token, or a way to identify yourself, or a credit card. And it also has built into the standard a way to encrypt all of this communication so that all of that data is transferred safely.

Bluetooth Connections

For higher speed and more persistent connections from our mobile devices, we might use a Bluetooth connection. We sometimes refer to Bluetooth as a PAN or a Personal Area Network. Bluetooth is used for many different mobile device connections.

We might use Bluetooth to tether our smartphone so that we can use it as a mobile access point. We might want to use our headphones or headsets over this wireless Bluetooth connection. Or we might want to connect health monitors or speakers so that we're able to communicate and send data to these devices without any wires connecting to our mobile device.

IR connectivity

On many mobile devices, especially Android devices, you may find that you have IR connectivity. This stands for Infrared. And although we used to use infrared for some limited printing or file transfer functionality, 802.11 has effectively replaced that. Where you'll instead find IR being used is in entertainment centers. So you can sit on your couch with your infrared-enabled mobile device and control your volume or the channel that's playing on your television

Mobile Devices Accesories (5:09)

https://www.professormesser.com/free-a-plus-training/220-1001/mobile-device-accessories-2/

TRRS Connector - Tip-Ring-Ring-Sleeve

I had said it's one of the most popular accessories for your mobile device. It allows you to put earbuds in your ear and have a microphone connected to the headset so that you can have both hands free to drive a car or perform any other function instead of holding the phone to your ear. Wired headsets commonly connect to a 3.5 millimeter TRRS connector. That stands for Tip-Ring-Ring-Sleeve. Sometimes you'll see this referred to as an analog audio jack.

Some iPhones don't have this analog audio jack. But they do have a lightning connector. So you can get wired headsets that plug into the lightning interface as well. If you have a Bluetooth headset, then you don't have to worry about any wires or any audio jacks. You simply connect your mobile device to the wireless headset using Bluetooth.

Here's a closer view of this TRRS connector that stands for Tip-Ring-Ring-Sleeve, where the connection at the end is the tip of the connector. And the connection closest to the other side is the sleeve connector. If you don't have a microphone, it's probably a TRS connector. But with the additional microphone, you have an extra connection in the middle for TRRS.

The speaker that's inside of our mobile devices are usually very small and difficult to hear. So it's nice to have an external speaker that you can connect. These are usually battery powered. And they connect to your mobile device over a Bluetooth connection. Because you can have these larger speakers, they're obviously easier to hear. And you get more of a stereo sound from these external speakers.

If you like playing games on your mobile device, you may find that that flat screen doesn't provide the best gaming interface. So you may want to use an external gaming pad. This looks very similar to a gaming console. But you can connect it to a phone or a tablet, usually over Bluetooth connectivity. And now you can use a traditional gaming controller to play games on your mobile screen.

External Power Sources

We know that our mobile devices rely on a battery source. And if we're running low on a battery, then we may have problems using this device over a longer time frame. If your device does allow you to swap batteries in and out, it's sometimes useful to carry an extra that's always going to be charged.

My mobile device doesn't allow me to swap out the battery. But I can connect to an external power source that allows me to connect through lightning or a USB connection. These external sources will be pre-charged. And then I can simply connect to the normal power connection on my mobile device and be able to charge that up very quickly.

Protecting Our Mobile Devices Screens

Our mobile devices have very large screens. And these screens can be easily scratched. So it's very common to get a screen protector that would go over that glass and protect it from being scratched.

You might also want to consider getting a protector that might go around the entire device, like this one. It's going to protect the entire device, both the front and the back, from scratches or breaking. There are also options to get cases that are waterproof, so you can protect it if you're out in the rain.

Your only problem might be if you want to plug this device now into a docking station, you may not be able to reach the interface on the bottom if this device protector is on it. This device protector might also create a conflict with wireless charging systems. So you want to be sure when you're buying a device protector that it does support wireless charging if that's a feature of your device.

Using Our Mobile Devices as a Point of Sale Terminal

Our mobile phones and tablets are powerful devices that connect to the internet so they can be used as a point of sale terminal. That means that you can accept credit card payments from your phone or from your tablet. These credit card readers might connect through the audio jack that's on your system. Or they might connect to the lightning port if you have an iOS device. There are also external credit card readers that connect to your phone through Bluetooth.

This means you can scan the magnetic stripe on a card. You can have someone insert their card so you can read the chip. Or you can accept an NFC transaction. Then your phone will use the internet, and you’ll get an instant approval for that transaction.

Your phone or tablet screen can also be used if somebody needs to sign for the transaction. And once the transaction is over, you don’t need to print a receipt. You can simply send it to someone’s email.

This is an example of one of the external credit card readers. There is a slot on the side that someone could insert their card. Or they can use this NFC connection to perform the transaction.

External Storage for Our Mobile Devices

There never seems to be enough storage space on our mobile devices. And if you have an Android device, you can increase the amount of storage by installing an SD or a micro SD memory card. Apple’s iOS devices don’t provide a way to increase the amount of storage. But many Android devices do support this removable memory.

If you have an older, larger device, it may support these SD cards. But you can see the micro SD cards are much smaller. And as our phones and our tablets are getting thinner and smaller, that may be a better form factor to use than this larger SD type of memory.

1.6 - Mobile Devices Connectivity 220-1001

Mobile Devices Connectivity (7:26)

https://www.professormesser.com/free-a-plus-training/220-1001/mobile-device-connectivity-2/

One of the big connectivity advantages of a smartphone is that it’s connected to the internet. It has data connectivity through your mobile provider. And that means that you could use that device to be able to connect other devices to the internet as well.

Make your Cell into an Internet Hotspot

One common way to do this is by turning your phone into a hotspot. You simply turn on the hotspot capabilities on one smartphone. And then everybody else who’s on that 802.11 wireless network can now use your phone to be able to get internet access.

This functionality and the amount of data you’re able to use over this connection is often managed by your wireless service provider. So make sure you check with them before enabling this capability.

Make your Cell into an Internet Hotspot for Yourself Only

If you’re the only one who needs this internet access through your smartphone, you can simply turn on tethering. This means you can connect your laptop to your mobile device using the USB connection. Or if your laptop supports Bluetooth, you can enable that and create your tethered connection over that Bluetooth link.

Once that tether is in place, you’re able to use the internet from your laptop by using the internet connectivity from your smartphone. Again, your wireless provider would be able to enable or disable this tethering feature. And there may be additional charges for tethering your laptop.

There are many different wireless networks that you can enable or disable on your smartphone.

- There’s, of course, your cellular network for communicating to your mobile provider.

- There’s 802.11 Wi-Fi network connectivity. There’s probably Bluetooth radio inside of your smartphone.

- And many smartphones also include near-field communication, or NFC networks.

Turning Off All Internet Networks in Your Cell

Many smartphones have an airplane mode that allow you to disable or enable all of these networks simultaneously. This way if you’re getting on an airplane and you need to disable all of these networks during takeoff and landing, you can click one button and everything will turn off. After takeoff if you then want to take advantage of the 802.11 wireless network on the plane, you can simply enable just the 802.11, and leave all of the other radios disabled.

Even if you’re not on a plane, you may want to have control over which wireless networks are in use. For example, if you’re not using Bluetooth devices, you may want to disable the Bluetooth functionality.

In iOS, you can go to the Settings to manually enable or disable these different networks, or use the Control Center that you can swipe down from the top of the screen and enable or disable the different networks from there.

There are many different ways to do this on Android. One common way is to go to Settings and then Wireless and Network Settings to be able to control what networks you’d like to use.

Bluetooth (personal area network/PAN)Connectivity Distance

Bluetooth is what we call a personal area network, or a PAN. It allows us to connect to devices that are in our local area, usually about 10 meters from us. So we can connect keyboards and headsets and speakers, all in our local area.

To be able to use this Bluetooth device, we have to initially pair with the device. So if you’re using Bluetooth in a car, you would pair with the car. Then when you leave the card and come back, the car and the phone will remember that they once paired together, and you don’t have to go through the pairing process again.

The pairing process is relatively straightforward. You would first enable Bluetooth on your smartphone and on the device that you would like to pair with. Then you would put those devices in discoverable mode. And you should see the devices show up on your screen that are able to be discovered.

Usually the name of a discovered device will appear on the other Bluetooth device. That way you know you’re choosing the right one. So you would then choose the name of the device you want to connect to. And usually a PIN will appear on both sides so that you can confirm that you have indeed selected the correct device. Once you’ve confirmed the PIN, you then choose to connect, and the devices are paired.

To be able to connect our smartphone to a cellular provider’s network, there needs to be a radio inside of this device that’s providing that communication. This is called a baseband radio processor. This is different than the Wi-Fi, Bluetooth, or NFC radios that are inside of your smartphone.

This one is specifically designed to communicate with the cellular provider’s network. It has its own firmware. It has its own memory. And even though you’re making phone calls over the cellular network, you really never see this particular part of the phone operating. This baseband radio processor uses a real-time operating system. This allows your phone to set a priority and be able to communicate over that cellular network.

The firmware associated with this baseband radio processor occasionally needs to be updated. And most often this update is occurring over the air, or OTA. You don’t really see this happening, although sometimes you may get a message that says that the radio has been updated for your cellular network.

One set of updates you might get are PRL updates. This is the Preferred Roaming List. These are common to CDMA networks, which are Verizon and Sprint networks here in the United States. These updates tell your phone which tower it should be communicating with. And usually these updates are provided over the air.

Another set of updates you might receive are PRI updates. These are Product Release Instructions. These have specific radio settings, like ID numbers, network codes, and country codes so that your phone knows exactly how to use the wireless network. These are also updated over the air. So you may never know that a PRI update has occurred.

Every mobile device on these wireless carrier networks can be tracked through a unique code called an IMEI. This is an International Mobile Station Equipment Identity code. Every smartphone has a different IMEI so your wireless carrier can allow access or disallow access based on this IMEI value. If you’re purchasing a phone, you may want to check the IMEI to make sure that it’s not locked. So when you receive the phone, it’s able to be activated on your carrier’s network.

A different type of identifier is an IMSI. This is an International Mobile Subscriber Identity. This is an identity that is associated with you and not with the mobile device. This IMSI could be provisioned in the SIM card, which means you can move the SIM card between different phones and still maintain access to your wireless provider’s network.

VPN (Virtual Private Network)

If you want a secure channel of communication between your smartphone and another device, you may want to enable VPN functionality. This stands for virtual private network. This creates a secure channel between your smartphone and another device.

The software you’d need to enable this VPN is often built into the phone operating system, although there is third party software you can install onto many phone operating systems that provide VPN connectivity.

This may require additional configuration on your side, for example, things like the VPN server that you’ll be connecting to, the account name that you’ll be using, whether you’ll be using an RSA secure ID token generator, and other requirements as well. Sometimes the VPN administrator will send you a single file that will then update your phone with the correct VPN details.

Configuring Email on Mobile Devices (7:00)

https://www.professormesser.com/free-a-plus-training/220-1001/configuring-email-on-mobile-devices-3/

POP3 and IMAP

Many of us use our smartphones and our tablets to send and receive emails. In order to do this, we have to configure these devices with the appropriate email settings for the type of service that we’re using. If you’re retrieving emails from an internet service provider’s email server, then you’re probably using the POP3 protocol or the IMAP protocol. If you’re sending mail from this device, you’re probably using the SMTP protocol for that particular ISP’s network.

Corporate Network Email Protocols

If you’re on a corporate network, you may be using something like Microsoft Exchange, which has a completely different process for sending and receiving emails. And if you’re using a number of providers that integrate email, such as Google, Yahoo, or iCloud, then there are a number of additional steps that you’ll need to take to be able to configure those accounts.

More POP3

Let’s start with a protocol that’s commonly used to retrieve email messages onto our mobile devices. This Post Office Protocol version 3, or POP3, is one of these protocols that’s been around for a very long time. We were using POP3 well before there was Yahoo, or Google, or Microsoft Exchange. This was the way that we would retrieve email messages from our internet service provider.

When we’re using POP3, we’re usually downloading an email message from our internet service provider’s account. And then you also have the option, when you retrieve that message, to delete that message from the server. This process of downloading a single email message and then deleting it from the server makes sense if you only have one device. And before we had smartphones, and tablets, and desktop computers, and laptop devices, and we were gathering our emails from so many different places, this type of protocol made a lot of sense.

But today, we don’t see POP3 used quite so often because we need more flexibility with how we’re retrieving and viewing our email messages. However, you may still find some legacy equipment or software that still uses POP3. So in those cases, we’ll need to provide configuration information into our smartphone to be able to retrieve these messages using the POP3 protocol.

POP3 using TCP port 110

We’ll, of course, need the name of the POP3 server. Usually there will be a hostname option for that. And usually there’s authentication that occurs to make sure that you’re the proper owner of those email messages. So you’d also provide a username and password into the POP3 configuration. The software you’re using may also require you to provide a port number that’s in use for this POP3 communication. This can normally be found from your ISP. And the default is for POP3 to use TCP port 110.

POP3S uses TCP port 995. (POP3 over a secure channel)

If you’re using POP3 over a secure channel– that’s a secure sockets layer encrypted connection, which is also known as POP3S– you’re probably using TCP port 995.

IMAP4 uses TCP port 143 (Internet Message Access Protocol version 4)

A more flexible protocol for retrieving email messages is the Internet Message Access Protocol version 4, or IMAP4. This protocol allows us to retrieve messages, but leave them stored on a central server. We have the ability to create folders using IMAP, and we can also perform searches on the server using this IMAP protocol. The configuration for IMAP is almost identical to the information you might need for POP3.

You, of course, need a name of the IMAP app server that you’ll be connecting to, and then you’ll need to provide a username and password. The ports that are used for IMAP are slightly different than POP3. If you’re using IMAP without any type of security, it’s usually using TCP port 143.

IMAP4 uses TCP port 993 (Internet Message Access Protocol version 4)

If you’re adding secure socket layer encryption, then you’re probably using TCP 993 to perform IMAPS communication.

SMTP uses uses TCP port 25 (Simple Mail Transfer Protocol)

We know that retrieving mail from your ISP is going to use POP3 or IMAP. But what about sending email messages? In those cases, we’re using SMTP, or the Simple Mail Transfer Protocol. This allows you to send email from your local device to your ISP’s SMTP server. Usually when you’re sending this message via SMTP, it needs to be from a device that can be trusted. So there’s usually authentication involved, and you have to make sure you configure figure all of those settings on your mobile device.

Although sometimes this authentication can be the same username and password that you use to retrieve email messages, it doesn’t have to be. So make sure that if you’re putting in SMTP authentication settings, that those match the SMTP settings that are configured on your ISP.

Most Authentication for SMTP runs over TCP port 587

And of course, SMTP uses a completely different set of port numbers than IMAP or POP3. If we’re performing a simple SMTP with no authentication, then we’re probably using TCP port 25. But most authentication for SMTP is going to run over TCP port 587.

For using email at home, being able to use POP3, IMAP, or SMTP probably works just fine for you. But at your office, you’d like to be able to integrate your email with a calendar. You want to be able to look up a set of contacts in a database, or have reminders provided on the screen. In those particular cases, you’re probably using an enterprise email system such as Microsoft Exchange.

Microsoft Exchange

Microsoft Exchange even allows the synchronization of this information, so you can keep a contact list on your phone and that same contact list is synchronized with Microsoft Exchange. The configuration options for Microsoft Exchange usually require that you provide an email address. You specify the Exchange server name. There’s usually a Windows domain name that needs to be configured. And of course, you need to authenticate with a username and a password.

Microsoft Exchange S/MIME Encryption

Microsoft Exchange also provides additional security for the email messages themselves. You can encrypt your emails using S/MIME. That stands for Secure Multipurpose Internet Mail Extensions. This allows you to both encrypt and digitally sign the messages that you’re sending and receiving from Microsoft Exchange.

You may not be retrieving mail directly from a server at your ISP, and you may not be using Microsoft Exchange. Instead, you may be using an integrated service, such as Google Mail or Yahoo Mail. And you may find on your mobile device, there are simply settings that you can click on to specify the email configurations for those individual services.

For example, if you’re using Google Mail, which allows you to split the inbox into multiple tabs and provide additional spam filtering, you can simply click the Google option and provide your Google authentication credentials. Google optionally allows you to retrieve messages using IMAP4 or POP3, but if there’s a built in Google configuration, you generally have additional functionality available.

The cloud-based service for Exchange is called Exchange Online, and there’s IMAP4 and POP3 support also available for that service. If you’re using iCloud from Apple, then you have Apple Mail support and IMAP4 support, as well. And Yahoo Mail supports not only the integrated Yahoo functionality, but you can also retrieve messages from Yahoo Mail using IMAP4 and POP3

1.7 - Mobile Devices Synchronization (5:15)

https://www.professormesser.com/free-a-plus-training/220-1001/mobile-device-synchronization-3/

Synchronization

In today’s mobile world, we have data that we’re spreading across many different devices. We have laptops, smartphones, and tablets, and desktop computers. And all of this data needs to be synchronized across all of these very different devices. We also have the need to be able to access any of this data from any of those devices at any time. And this doesn’t refer to any single type of data. We need to be able to access all of our email messages, our photos, our movies, our text messages, and all of this data from all of these devices.

We also have to make sure that all of these devices are constantly synchronized. We’re moving from one device to the other. And we need to be sure that, no matter what device we’re using, we have access to exactly the same data. The security to protect this data is also important. So our mobile devices not only need to authenticate to the servers, the servers need some way to prove that they’re talking to our personal devices.

Here’s a summary of just some of the data that we tend to synchronize between all of these different devices– our contact lists, the applications that we use, our email messages, bookmarks, documents, books, and even our passwords are now shared amongst all of our different mobile devices. If you want a hands-off way to synchronize all of this data, you would synchronize to the cloud. You wouldn’t have to plug-in a cable to synchronize to a desktop computer. And this may be a process that’s integrated into an existing mail system that you’re using.

For example, Microsoft Exchange will synchronize your contact lists, your emails, your calendar settings, and so much more. If you’re using Apple’s iOS operating system on your mobile device, you can sync all of this data to Apple’s iCloud. It provides a backup and recovery process so if something happens to your mobile device, you can simply purchase a new device, put in your iCloud credentials, and the device will download all of your information and update that new device.

For Android, cloud-based synchronization is provided through Google. So you would log into your Android device with your Google credentials. And that’s what will provide the synchronization to your Google account. If you prefer not synchronizing to the cloud or you don’t have access to be able to do that, you can always synchronize to your desktop computer. This means that you would need to use an application on your desktop that supports this synchronization. And you have to make sure that you have enough disk space to store all of this data that’s from your mobile devices.

Backup Storage

For example, if you're using Windows or Mac OS, then you can use Apple's iTunes to be able to synchronize your iOS devices. Fortunately, these applications don't require an extensive amount of storage and memory. But they do require an extensive amount of storage on your storage device. So your hard drive or SSD will be backing up and storing all of this data from your mobile device. This could be gigabytes in size, so you have to make sure you have enough free disk space.

Apple Devices Backups

Apple provides iTunes to make backups of your iOS devices. And it creates a complete backup on your computer. If you get a new iOS device, you can plug-in your computer to this device and iTunes will restore everything to that new iOS device.

Android Devices Backups

If you have an Android device, there is no built-in process for storing information on the desktop. By default, everything is stored in the cloud. There are some third party applications, such as doubleTwist, that allow you to transfer movies or music to and from your Android device.

Automobiles Backups & Accessing our Devices

We spend a lot of time in our cars. And our automobiles are becoming more aware of our mobile devices. You're now able to plug in a cable or use Bluetooth to extend your phone functionality into the car itself. Many cars can also provide additional enhancements that allow you to share contact information, view maps, play music, and perform other functions from your mobile device. If you have an iOS device, then your car may be able to use iOS CarPlay to perform this functionality. Android has a similar feature called Android Auto.

By using these enhanced features, our car is now able to see our contact list and be able to integrate and control our phone, all from the car's console. This, of course, is something you should be aware of, especially if you're using someone else's car, because all of your contact information can then be transferred into your car. And then the next person who uses the car might be able to see your personal information.

Automobiles & Devices Synchronization

To synchronize information on your mobile device, you either need to connect a cable or use a wireless network connection. Normally, you're plugging into a wired connection on your computer, using this USB standard type-A connection. If you have an iOS device, you may be able to connect with Apple's proprietary connectors. Older iOS devices use the Apple 30-pin connector. But newer iOS devices might use the Apple 8-pin lightning connector or the more standardized USB-C connection.

Most mobile devices can also communicate over 802.11 wireless networks. And if your device supports it, you can communicate over a cellular wireless network. On Android devices, you can synchronize over USB Micro-B or USB-C. Or you can use your 802.11 wireless network or the network from your mobile provider.

****

A+ 1001 Section 2: Networking

****

2.1 – Ports and Protocols

Introduction to IP (12:09)

What is the TCP/IP Protocol used for

TCP/IP is one of the most popular protocols in use today. And in this video, I'll give you an overview of how IP is used on today's networks. If you need to move the contents of your house from one place to the other, then you would probably use a moving truck to do that.

It’s a similar idea for moving data from one side of the network to the other. We have a road that’s built, which is our network. It’s an ethernet network or a cable network or a DSL network. And on this network, we put a moving truck. This truck is TCP/IP, or the Internet Protocol for short. We have specifically designed these roads to be able to transport this specific kind of moving truck.

Inside of the moving truck is all of our belongings or our data when we’ve separated this data into UDP data and TCP data. We’ll talk about those two types of data in just a moment.

What is being send using TCP/IP protocol

Inside the boxes, of course, are even more of the things that we own. That’s more of the application data and the information that we’re sending from point A to point B. In reality, we don’t usually have multiple boxes inside of our moving truck. We’re usually on an ethernet network that is sending data using IP, which is using TCP, which has application data inside of that.

If we were to visualize how this would look going across our network, we would have a client on one side sending information to a server on the other side, and it would be sending this information using an ethernet frame. Inside of this ethernet frame is a header at the beginning of the frame and a trailer at the end of the frame. And in the middle is what we call our ethernet payload.

Inside of this ethernet payload is an IP header, which is followed by an IP payload. We can break out our IP payload into perhaps a TCP header, which has its own TCP payload. And ultimately, what’s inside of that TCP payload is application data. For example, HTTP data that’s being sent to a web server.

Information Nesting

With this nesting of information, we have ethernet, which has IP. And inside of IP is either TCP or UDP. We call this an encapsulation of protocols as we begin putting one protocol within another within another. This gives us a couple of ways to move data from one side to the other. We can put information into a TCP box, or we can put information into a UDP box. There are different features for the different protocols, depending on the type of application that we’re using.

What OSI Layer is Used by TCP/UDP

You might also see this referred to as an OSI layer reference. In the case of TCP and UDP, this operates at OSI layer 4. This idea of being able to put multiple applications inside of different frames and send them all across the network at one time is a concept we call multiplexing, and allows us to perform many different functions simultaneously over the same network connection.

TCP vs UPD

TCP - How Does it Work

Let’s look at the differences between the TCP protocol and the UDP protocol. Let’s start with TCP. It stands for Transmission Control Protocol. We refer to TCP as a connection-oriented protocol, which means there is a formal process when you start the communication and a formal process when you end the communication.

You can think of this as making a phone call. You type in the numbers on your phone. You hit Send. When someone answers, you say, hello? And then after that point begins the conversation. At the end of the conversation, both sides say goodbye, and you hang up the phone.

It’s similar to how TCP operates. You might also see that TCP is called a reliable form of delivery. We call it reliable, because if any errors occur during that communication, there’s a process for retransmitting that data to make sure that everything gets through the network without any problems.

The way that TCP is able to resend data or slow down or speed things up is that there is an acknowledgment every time data is sent. So if station A is communicating to station B and sending some data, Station B will always respond back that it received the data without any problems. If station A does not receive an acknowledgment, then it assumes that data didn’t get through, and they can resend that data to the other side.

UDP - How Does it Work

The UDP protocol is the User Datagram Protocol. This is a connection list protocol. There’s no formal call setup. Data simply is sent through the network, and it arrives on the other side without any hellos or goodbyes.

We also consider UDP to be unreliable in its form of delivery. This doesn’t mean that the data has any more or less chance of making it to the other side. It only means that there’s no acknowledgment to the data. So station A will send data down to station B, and station A will never receive an acknowledgment that that data is received. UDP doesn’t provide any acknowledgment.

This doesn’t mean that UDP works any better or worse than TCP. Different applications use different protocols for different reasons. There might be an application that doesn’t need any type of acknowledgment that information was received, so it sends it through the network without any type of receipt that it was received at the other end. Some applications really want to be sure the data gets through, and in those cases, those applications may use TCP so it effectively gets a return receipt of that information being sent through the network.

IP Ports - Sending and Receiving Data to Sockets

Now that we’ve looked at the data that we put inside of our TCP box or our UDP box, let’s look at how we get the box from one location to the other. The way that we do that is using IP, the internet protocol. Just as every house on your block has a different street address, every computer on the internet has a different IP address. So we can send information from one IP address to the other, and we know exactly where it’s going.

Once the boxes arrive at the house or the IP address that we’ve sent it to, we need to know which room in the house we’re going to put that box. As the movers are coming in, someone is going to be looking at the box, seeing what’s labeled, and then sending that mover to the correct room of the house.

For example, the boxes may arrive at the house. They may be marked bedroom, living room, kitchen, or bath. And now you know exactly where that box goes inside of that house.

With IP, the process is similar, but instead of using a room name, we use what’s called a port number. This way, we can send information into a server and we know exactly which service on that server needs to receive that data.

For example, a box of data arrives at this house. There’s many different services running inside of that server. And some of the data will go to port 80. Some of the data will go to port 443. Other boxes of data will go to port 123, and other services will provide access over port 25.

What is an IP Socket

Putting these all together then, we have what's known as an IP socket, which means we have a server's IP address. We have a protocol such as TCP or UDP, and we have a port number that's used. The same thing applies on the client side. We can have a client IP address, a protocol, and a client port number. All of these together would be IP version 4 sockets.

To be able to communicate this way, we need to be able to use many different port numbers all at the same time. There are different types of port numbers. One type is a non-ephemeral port. Ephemeral means temporary, so these would be non-temporary ports, or permanent port numbers.

These are usually port numbers that are assigned to an application. This would usually be a port number assigned to an application. Very commonly, these non-ephemeral ports are numbered 0 through 1,023. For example, a web server may be using TCP port 80. That would be a non-ephemeral port associated with that web service on that server.

**** TODAY WE HAVE 65,535 PORTS ****

Just as we're communicating to the server using the server's port numbers, the server also has to communicate back to the client using the client's port numbers. A client is usually choosing a random set of port numbers between 1,024 and 65,535. These port numbers are used only for that session. They are temporary port numbers, or what we call ephemeral ports. And they're usually chosen at random by the client so that it's able to send information to the server, and the server would have a way to get that information back to the client.

This means we have a wide range of port numbers that we could use. We could have a TCP port number range between 0 and 65,535. We could also have a UDP range of port numbers between 0 and 65,535.

If we're communicating to a server then, we're probably using a non-ephemeral port number, and it's probably a port number that's in the range between 0 and 1,023. But you may find that some servers use different port numbers that are outside of that range, and that's perfectly fine. These numbers are just a way to signify what room that particular data goes to, and there are no hard and fast rules over what port number an application happens to use.

That's because these port numbers are used for communication. They're not a security mechanism. We don't decide on the port number based on any type of security requirement. We're simply setting the port number so that we know where to send the data.

The one thing that is important about the port number is that the client that you're using needs to be able to know the port number that's open on the server. For example, if you're using a web browser, the web browser expects that the web server is going to be using TCP port 80. If that web server is using any other port, than your browser by default will not be able to communicate to that server, and you would have to specify inside of your browser to use a different port number on that server.

As you can imagine, that becomes more complicated if everybody gets to decide a different number for their web servers. That's why we've centralized on everyone using a well-known TCP port 80 so that everyone's browser knows exactly how to access all of the other web servers on the internet.

Are TCP and UDP ports the same

Also keep in mind that TCP port numbers are not the same as UDP port numbers. There could be an application running on a server using TCP 80. There could be another application on that same server that uses UDP 80, and neither of those applications will be communicating with each other.

Here's a practical view of how this might work. We have a client on one side that has an IP address of 10.0.0.1. We have a server on the other side that has an IP address of 10.0.0.2.

There's three application communications that are taking place. One is a web server that communicates on TCP port 80 on the server. There’s also a voiceover IP service running on that server that uses UDP port 5,004. And that server also provides an email service on TCP port 143.

If the client needs to communicate to the web server that’s on that service, then it knows it needs to send from 10.0.0.1, the IP address of the client, to 10.0.0.2, the IP address of the server. We also know on the server that our destination port number is going to be TCP 80.

But for this client to be able to communicate to that server, it also needs to randomly choose a port number that it can use to begin the communication. And in this case, the client has chosen TCP port 3,000. When the client sends data to the server, the server knows to send the data back to the client using that port number as the destination as it goes to the other direction.

At the same time, this client could be communicating to that server over voiceover IP using UDP port 5,004. You can see that’s the destination port in that second frame. And you can see that randomly, that client chose UDP port 7,100 to communicate for this particular flow.

And lastly, we can see that the client is also sending email communication to that server, sending it to TCP destination port 143. And the client has chosen the random TCP port number of 4,407 to be able to send that email communication to the server

Common Network Ports (9:53)

FTP (File Transfer Protocol) Purpose

One of the first ways to transfer a file from one device to the other uses a protocol called FTP, a File Transfer Protocol. This protocol uses TCP port 20.

We call this the active mode data port, and there is a TCP port 21 that’s used to control the communication.

TCP does have security built in, so you can configure a username and a password that gains access to another system.

FTP also supports a mode called anonymous log in where you can use the user name anonymous and then any password you’d like. As it transfers files, FTP provides what could be called full featured functionality. You can list the files available on a system. You can add files, delete, rename, and provide other file functions as well.

SSH (Secure Shell) Purpose

If you’ve ever communicated across the network to another device at the command line, then you’ve probably used a console connection that looks very similar to this one. If your console connection is over an encrypted channel, then it’s probably using SSH or Secure Shell over TCP port 22. Although this looks very similar to a console screen you might see if you use Telnet, Telnet would be over a nonencrypted channel, but SSH always uses an encrypted communication link.

Telnet (Telecommunication Network) Purpose

You may find that some older equipment doesn’t support SSH and the only way to communicate to this device and use this terminal communication is by using Telnet. Telnet stands for Telecommunication Network, and it uses TCP port 23. Just like with SSH, we would use Telnet to log in remotely to this device at the console, but we have to keep in mind that this entire communication is in the clear. There’s no encrypted communication.

So if you type in your username and password, anyone capturing those packets on the network is able to view very plainly your user name and your password. For that reason, we don’t commonly see Telnet used on anyone’s network. And if you need to keep your system secure, you would probably only use SSH, instead of using Telnet.

In an earlier video, we talked about mobile devices sending email messages and the protocol that it used to send those messages was SMTP or the Simple Mail Transfer Protocol. SMTP can be used to send messages from a mobile device, or it can be used to send messages from one server to another. SMTP uses TCP port 25 to be able to send that data. If you’re receiving email messages, you’re probably using POP3 or IMAP. Whenever you’re sending email, it commonly uses SMTP.

DNS (Domain Name System) Purpose

If you’re typing a website into a browser, you’re probably using the name of the site. So if you type in www.professormesser.com, behind the scenes, there needs to be a conversion between that domain name and the IP address of my web server that’s where we would use DNS, which communicates over UDP port 53. This is converting those names to IP addresses and then back again. For example, if you type in in www.professormesser.com, that information is sent to a DNS server, which responds back with an IP address that’s associated with my web server.

We obviously rely on these DNS servers to be able to provide this resolution between domain name and IP address. And since we’re using mostly these domain names and we’re typing things in at a browser, we’ll probably have multiple DNS servers. So if we happen to lose a DNS server or it happens to become unavailable, we have other DNS servers that can provide that resolution.

There are two types of DNS systems. The external DNS which is connected to the Internet, and the internal or private DNS which is used in private networks.

HTTP (Hypertext Transfer Protocol) vs HTTPS (Hypertext Transfer Protocol Secure)

If you’re in a web browser and you’re communicating to a web server, then you’re probably using HTTP or HTTPS as those protocols.

HTTP stands for Hypertext Transfer Protocol, and HTTPS is the encrypted form of that or Hypertext Transfer Protocol Secure.

These two protocols used two different port numbers to communicate.

The in the clear, non-encrypted version of HTTP uses TCP port 80.

The encrypted communication occurs with HTTPS and that commonly uses TCP port 443.

POP3 vs IMAP Ports

If you’re on a mobile device or desktop computer and you’re receiving emails, then you’re probably using POP or IMAP as those protocols. POP3 is the Post Office Protocol version 3. It uses TCP port 110, and it provides basic mail transfer functionality. Many of our modern mail transfers are using IMAP.

IMAP is the Internet Message Access Protocol version 4. It uses TCP port 143 to communicate. IMAP provides some enhanced features over POP3, such as having multiple folders and being able to access that email box from multiple devices.

Windows RDP (Remote Desktop Protocol) Purpose

If you’ve ever needed to view or take control of someone’s desktop across the network, then you’ve needed to use RDP or the Remote Desktop Protocol. This uses TCP port 3389 to provide that remote control functionality. You’ll find that RDP is available on many different Windows servers and allows you to either view the entire desktop of the remote system or view just a single application that’s running on that remote system.

There are many different clients available to access these remote desktop services. You can run it on a Windows workstation, Mac OS, Linux, and many others. Microsoft Windows doesn’t use FTP to transfer files from one system to another. Instead, it uses its own format to be able to transfer files called server message block.

*** FTP runs on Windows as well ***

This is a standard set of protocols that Windows uses that allows for file sharing, printer sharing. You might even see it referred to as CIFS or Common Internet File System. Older Windows systems may use NetBIOS that is inside of a UDP or TCP packet.

UDP port 137 is NetBIOS name services so that you can find the device on the network by its name. There’s also UDP port 138, which is the NetBIOS Datagram service. There’s a TCP version of this that runs on TCP port 139, which is the NetBIOS session service.

Modern Windows devices don’t need to parse out these different NetBIOS protocols and put them inside of TCP or UDP. Instead, they can communicate directly over TCP port 445. Just as Windows has its own protocols for transferring files, Mac OS also has its own protocols for the Apple Filing Protocol or AFP.

These file services in Mac OS use TCP port 548. To be able to view the list of available servers, you’re probably going to use the service location protocol in Mac OS or SLP. The service location protocol uses TCP port 427 and UDP port 427 to be able to populate a list of available locations. And very similar to SMB in Windows, the Apple filing protocol in Mac OS is also full feature. You have the ability to view the available list of files to copy files, move files, rename files, and more.

DHCP (Dynamic Host Configuration Protocol)

When you turn on your computer for the first time, it automatically configures itself with an IP address. It’s able to do this because it’s using DHCP, which is the Dynamic Host Configuration Protocol.

There is a DHCP server somewhere on your network, and your client communicates that server using ports UDP 67 and UDP 68. Once your workstation receives this IP address, it’s available for a particular lease time.

And before that lease is up, it has to check back in with the DHCP server to make sure that it’s still able to use that IP address. The DHCP servers can also be configured with DHCP reservations. This means when a workstation or a server requests an IP address, the server can recognize the MAC address of that device and provide the same IP address to that device every time.

If you connect to a corporate network for the first time, you’re often asked to provide a username and password. The same thing occurs if you connect through a VPN or if you log into a web server that’s on the network. The process of providing that authentication is usually to a centralized database, and one very common form of database that’s used for this is LDAP.

This is the Lightweight Directory Access Protocol, and it uses TCP port 389 to provide that authentication. This means that you can’t store all of your credentials in one single database. And if you ever need to enable, disable, or make any changes, you simply need to make it in that centralized location.

Network administrators may have tens or hundreds or even thousands of devices they have to manage on a single network. In order to constantly monitor and gather statistics from these devices, these network administrators use a specialized protocol called SNMP. This is the Simple Network Management Protocol, and it uses UDP port 161 to query devices, and it can receive alarms or traps from those devices over UDP port 162. There may be three different versions of SNMP that could be running in an environment.

Version one was the original that provided a non-encrypted, in the clear method so that a device can communicate to a router and ask how many bytes have gone through a particular interface, and that router can respond back with that value. Version 2 of SNMP still communicated without any encryption, but this client could ask many different questions at the same time and receive a bulk transfer in response. Many organizations these days are using SNMP version 3, which provides message integrity and authentication method. And all of the information that’s sent between the client and the remote device is all encrypted.

Ports

A port is a logical network location where a specific process or a type of network service is executed.

A service is an application running at a specific network port

Port	Type	Name
20	TCP	FTP, a File Transfer Protocol.
21	TCP	Controls the FTP communication
22	TCP	SSH or Secure Shell, always encrypted
23	TCP	Telnet (Telecommunication Network) never encrypted
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	UDP	DNS (Domain Name System)
80	TCP	HTTP (Hypertext Transfer Protocol) non-encrypted
443	TCP	HTTPS (Hypertext Transfer Protocol Secure)
110	TCP	POP3 (Post Office Protocol version 3)
143	TCP	IMAP (Message Access Protocol version 4)
3389	TCP	Windows RDP (Remote Desktop Protocol)
137	UDP	NetBios (Finds a device on the network by its name)
138	UDP	NetBIOS Datagram service
139	TCP	NetBIOS Session Service
445	TCP	Modern Windows devices can communicate directly
548	TCP	AFP (Apple Filing Protocol)
427	TCP	SLP (Service Location Protocol in Mac OS) and
427	UDP	SLP (Service Location Protocol in Mac OS)
67	UDP	DHCP (Dynamic Host Configuration Protocol) and
68	UDP	DHCP (Dynamic Host Configuration Protocol)
389	TCP	LDAP (Lightweight Directory Access Protocol)
161	UDP	SNMP (Makes queries. Simple Network Management Protocol)
162	UDP	SNMP (Receives alerts. Simple Network Management Protocol)

2.2 – Network Devices

Network Devices (17:30)

NICs (Network Interface Card) Types

As an IT professional, you’ll be working with many different networking technologies. So in this video, we’ll look at some of the most common network devices. If you are connecting a device to a network, whether it’s a wired network or a wireless network, it needs some type of hardware to be able to make that connection. We call this piece of hardware a Network Interface Card, or a NIC.

So you will find a NIC inside of your printers and your servers and your laptops and your workstations and anything that needs connectivity to a network. The network interface card that you’ll be using will be specific to the type of network you’re connecting to. So if you have an ethernet network, then you will need an ethernet NIC.

If you have a wireless network, you will need a wireless NIC. And if you are connecting to multiple types of network, you will need multiple types of NICs inside of your device.

The network interface card that’s here is an external adapter you would plug into the motherboard, but many motherboards have a network interface card built into the motherboard itself.

There are also many other types of network interface cards. This one happens to be a copper ethernet interface, but you can get network interface cards that have fiber connections, Wide Area Network connections, multi-port connections, and other options.

Repeaters

If you’ve ever had to extend a network connection over a very long distance, you know there is a maximum link that is supported for that particular topology. One way that you can extend this link to be even larger is to use something like a repeater. A repeater receives a signal, regenerates it, and then resends that signal out another interface. It doesn’t have to make any forwarding decisions. It doesn’t have to decide which connection this is going to. This is a simple goes in one connection and goes out of another connection.

It’s very common to use these repeaters to extend the length of a network. So we might be extending a fiber network, or we might be extending a copper network. Or it might be the situation we have with this repeater where we’re converting from one physical type to another. For example, we’re coming in at 100 megabit ethernet over fiber, and we’re outputting this repeater at 100 megabit ethernet over copper.

HUBS

In the early days of networking, if you had to connect a lot of different devices together, you might use something like a hub. This is an ethernet hub. This is a very small ethernet hub with only four interfaces on it. But these hubs could be tens or even hundreds of interfaces in size.

The way that these hubs operate is that information that is sent to one interface on this hub is automatically repeated to every other interface on this hub. This is very similar to the functionality we saw with repeaters, but the repeater was only repeating it out a single interface. With a hub you’re, repeating it out of multiple interfaces simultaneously. You will sometimes hear a hub referred to as a multi-port repeater.

The communications process on a hub all occurs at half-duplex because of this repeating functionality. This means that two devices can’t communicate at the same time on a hub. You can have one device sending traffic. Once that device is done, another device can then begin sending information.

If you don’t have a lot of devices on the network communicating to each other, then this half-duplex functionality is just fine. But as more devices begin communicating, the efficiency of the network begins to decrease. Ethernet hubs only operate at 10 megabits per second or 100 megabits per second. You won’t find any gigabit speed hubs. In fact, it’s hard to find 10 or 100 megabit hubs today, because the technology doesn’t scale as you put more traffic on the network.

In these early networks where we used hubs to connect all of our devices, we would connect the hub networks together by using a bridge. These bridges make decisions on what traffic should be forwarded through the bridge based on the destination MAC address that’s inside of that ethernet frame. That certainly sounds very familiar, because that’s the same type of forwarding decision made by today’s modern switches. But back in the day, these bridges only had two or maybe four interfaces available to be able to make those forwarding decisions based on MAC address.

Bridges and Switches

These bridges allowed us to make networks that were a bit smaller so that each one of these hub networks was able to operate efficiently. And sometimes we would use these bridges to switch between different topologies. So we could move from an ethernet network to a WAN network by sending that traffic through a bridge. Instead of making traffic decisions like a hub which took traffic from one interface and repeated it to all of the other interfaces on that hub, the bridge was a little more intelligent with how it would decide where traffic was going. It would look at the destination MAC address, find out what interface on the bridge that destination MAC address existed, and then would send that traffic to only that interface where it was destined.

A good example of a modern version of a bridge would be a Wireless Access Point where you have a wireless network on one side, and on the other side, it’s connecting to your wired ethernet network. That wireless access point is performing a bridging function. So it’s looking at the destination MAC address of the traffic it receives, and it’s deciding whether it should send it on to the wireless network or whether that traffic should go onto the wired network. These days, we’ve extended this idea of bridging into very large scale systems that have hundreds of ports on them or are making these forwarding decisions in the hardware of these devices. We call these newer style bridges switches, and we’re able to support huge infrastructures with hundreds of devices on a single switch by using this switching technology.

The switches are performing exactly the same function that these bridges did. It’s looking at the destination MAC address, and it’s sending that information to the appropriate interface on that switch. It’s able to do this very, very fast across hundreds of different interfaces by performing this switching look up in hardware. This switching hardware is an Application-Specific Integrated Circuit, or an ASIC. And it’s this hardware switching that allows us to scale this up to hundreds of interfaces on a single switch.

If you look at the core of an enterprise network, you’ll probably see a switch like this with hundreds of interfaces on it, or it may be a smaller switch that’s in a networking closet on another floor or used in a small office or home office. As we mentioned earlier, these switches make their forwarding decisions based on the destination MAC address of the traffic going through the switch. As we’ll find out later in this video, if a device is making its forwarding decision based on the destination IP address of the traffic, then that is a router. There are some switches that allow you to have both switching functionality and routing functionality within the same device. We refer to these as multi-layer switches or layer 3 switches.

Un-managed Switches

If you’re installing a network switch and you need very basic functionality, then you’ll probably want to use an unmanaged switch. There’s not a lot of configuration involved with setting up an unmanaged switch. You simply turn it on, plug in all of the devices, and they can all communicate to each other. There’s usually not even a configuration tool or utility you would use to configure the switch. You simply connect all of the devices, and they would all communicate across the same virtual LAN.

This also, obviously, would not integrate with other external protocols. If you needed this switch to be able to communicate back and forth to a management station via SNMP, then you probably wouldn’t use an unmanaged switch. The trade off, of course, is that the cost of the switch is lower if you don’t have to support all of these other features. So if all that you need is basic connectivity at a low price point, then you may want to consider an unmanaged switch.

Managed Switches

Many organizations, though, need additional functionality in their switches. And in those cases, they would purchase and install a managed switch. Managed switches allow you to configure different VLANs on different interfaces, for example. You might also be able to connect switches together in a trunk. You might also hear those referred to as 802.1Q.

There might be traffic prioritization on the switch so you can decide what types of traffic have a higher priority than other types of traffic. There’s also some redundancy support you may be able to configure in a managed switch by using Spanning Tree Protocol. And our network management station can communicate to these devices using a specialized protocol called Simple Network Management Protocol, or SNMP. And for people that need to do troubleshooting on the switch, you can set up port mirrors, so traffic can be mirrored from one port to another. This allows you to connect a network analyzer to one of the ports on the switch and copy traffic from any other port on that switch to watch the traffic flows across the network.

Routers

A device that makes forwarding decisions based on a destination IP address is a router. These are usually standalone devices, but sometimes that routing functionality can also be integrated into switches. We usually refer to those as multi-layer switches or layer 3 switches.

It’s also very common to use routers to connect different types of topologies. So we may connect a serial WAN link, an ethernet copper connection, and an ethernet fiber connection all on the same router. Many organizations provide access to wireless networks by using a Wireless Access Point, or a WAP. Although these wireless access points look very similar to the wireless router that you might use at home, the operation of these devices is quite different.

The wireless router, you have at home is not only a wireless device. It’s also a router switch. It has other functionality as well. In comparison, a wireless access point is simply extending a wired network onto a wireless network and allowing connectivity between those topologies. A wireless access point is making its decision based on the destination MAC address. Therefore, it’s acting also as a bridge.

If you walk around a large facility such as a hospital or a university, you’ll notice there are a large number of wireless access points as you move from building to building. And of course, someone has to manage all of these wireless access points on the network. To be able to centralize this management, these organizations use a wireless LAN controller. This allows you to have a central management console to be able to support hundreds or even thousands of wireless access points wherever they happen to be on your network.

If you need to deploy a new access point, change the configuration, update software, or anything else associated with the management of that device, you would use one of these wireless LAN controllers. This is usually a proprietary system. So if you have a Cisco access point, you’re probably using a Cisco wireless LAN controller.

Although we’re showing a physical device here to represent a wireless LAN controller, there is some wireless LAN control software that runs in the cloud. So you can simply connect to the cloud-based controller from anywhere you happen to be able to manage all of those access points on your network. Many organizations use firewalls to be able to manage the control of traffic flows through their network, especially traffic flows that are going to or coming from the internet.

Firewalls

A traditional firewall allows you to filter information based on the UDP port number or the TCP port number. You may sometimes see this referred to as OSI layer 4 filtering. But modern firewalls are able to examine everything in that traffic flow, including the application that’s in use. So a security administrator can tell the firewall to allow database transactions but prevent file transfers through the network.

Many firewalls also rely you to create encrypted tunnels to and from that firewall. So if you’re off site, you still need connectivity to the corporate network. You can connect over a secure channel to the corporate firewall and then be able to communicate to your internal resources. You might also even find older firewalls that act as a proxy, which means that they sit in the middle of the communication.

If you wanted to surf a website, you would send that request to the firewall. The proxy firewall would then make the request for you, receive the response, check through the response, and make sure it’s appropriate for you to view and then send that traffic to you. It’s also common to see many firewalls used as a router. Sometimes you’ll see this referred to as an OSI layer 3 device. These routers are able to also sit on the edge of the network and be able to do any type of routing or network address translation based on the routing engine inside of the firewall.

Cable Modems

A common network device on both home and corporate networks are cable modems. These allow you to connect to a broadband network, usually provided by a cable television company, that is sending data across the network using a standard called DOCSIS. That’s Data Over Cable Service Interface Specification. These DOCSIS networks support many different types of throughput. You can have slower networks at four megabits all the way through his higher speed networks at 250 megabits per second. And these days, it’s not uncommon to see gigabit networks running over these cable modem networks.

Another important aspect of these DOCSIS networks is the support for multiple services. We’re already supporting video through this network, and now we’re including the data for our internet connection and telephone communication with voice as well. For both home and business networking, DSL is a viable competitor to the cable modem networks. Instead of using the same cable used for cable television, a DSL network is going to use the same wire that we traditionally use for our telephones. DSL stands for Digital Subscriber Line, and you’ll sometimes hear it referred to as Asymmetric Digital Subscriber Line.

It’s asymmetric because the download speed that you receive on DSL is faster than the upload speed, making it an asymmetric communication. One challenge we find with DSL is there is a significant distance limitation between the telephone company's central office and the telephone jack that's inside of your home. The maximum distance you would be able to get on DSL is somewhere around 10,000 feet.

If you live close to the central office, your throughput will be faster than someone who lives farther away from the central office. DSL speeds generally range around 52 megabits per second downstream and 16 megabits per second sending traffic upstream. And if you live closer to the central office, your DSL connection may even be able to support faster speeds than that.

Patch Panel

This is a picture of a traditional company's network configuration on the floor of the building. You've got a lot of people out on the floor that are working at their desk, and all of these devices have wires, ethernet cables, that go into the ceiling or under the floor into one of the closets that's somewhere nearby. And in that closet is a patch panel. This patch panel terminates those wires onto what we call a 110 block and provides, inside of that closet, a set of RJ45 connectors that go all the way back to each person's individual desk.

Also in that closet, we have our networking equipment. So we're able to create a simple patch between our patch panel and our networking equipment by simply extending some ethernet patch cables inside of our closet. This patch panel also allows us to make changes very easily. We can simply extend a connection. And if we realized we wanted to connect that user to a different switch, we can simply move the wire down to a different switch.

If they're on a different VLAN or a different network, then we can connect those users to a different switch or a different set of interfaces on the same switch. This means you only have to punch down all of the wires from everyone's desk one time. If someone then moves from one desk to another or we need to plug that person into a different type of network connection, we simply disconnect the cable inside of our closet and plug it into the new connection.

We don't need to run a new cable from someone's desk. We don't need to use any special tools inside of our closet. We simply connect and disconnect using the RJ45 interfaces on the patch panel and on our networking equipment.

Traditionally, if you were installing a wireless access point, there would usually be two connections for that wireless access point. One connection was to provide the network connectivity for the access point. The other connection was to provide the power, and then we would need to plug into a power outlet to be able to power that access point. Today, we're providing that power over the ethernet cable itself. We call this Power over Ethernet, or PoE.

Power over Ethernet (PoE)

This means that we can run a single cable now to our wireless access points, to our phones, to our security cameras, and we don't need any additional connections to be able to power those devices. The power that we have on a PoE connection is often coming directly from the switch, and you have a single run all the way to that device. In those scenarios, we call that an endspan. In some cases, you may need to install a device that requires a PoE connection, but your switch does not provide any power.

In those cases, you can put a device in the middle, like this PoE injector, which adds power to the ethernet connection so that you can then power that device. Most switches that support power over ethernet will say it on the switch itself. For example, this is a 10-point gigabit power over ethernet managed switch.

Power over ethernet allows us to power device using our ethernet cables. Ethernet over Power, or EoP, is the reverse of that where we are extending our ethernet network using the power cables that we already have in our home. You might also hear this referred to as PLC or Power Line Communication. And it's an IEEE standard numbered 1901. This EoP standard operates at 500 megabits per second, and it's designed to connect devices that normally wouldn't be connected to our ethernet. Networks for example, if we had an electric car that we recharged overnight, when we plugged it into the power source, it would also be connected to our ethernet network.

2.3 – SOHO Networks

Installing a SOHO Network (6:09)

If you work in a large corporation, you probably have a data center, and that data center has many racks of equipment. You have routers and switches and firewalls and intrusion prevention systems and many other components that make up your networking infrastructure. But if you’re in a small office, home office, that’s a SOHO, you don’t have room for all of these devices.

And a lot of this functionality can be collapsed down into one single device, and that would be the SOHO router. This is the SOHO router that I use for my studio, and you can see it’s a single device. But there’s a lot of functionality inside of this one device. It connects to my Comcast cable modem network.

There’s connectivity on the back for Ethernet. There’s also connectivity on the back for telephones. All of these interfaces on the back are switched. There’s a firewall inside of this.

There’s a wireless access point. And so a lot of functions are inside of this single all-in-one device. Your SOHO router is going to have routing functionality that connects the outside world– usually, over a DSL connection or a cable modem connection. And this is what’s going to allow you to route between your internal private network and the external internet network.

SOHO routers also very commonly have a switch built in to them. This one has four individual interfaces. It’s a single VLAN, and you have four devices that you can plug in with an Ethernet cable.

One of the advantages behind the design of these SOHO routers is there’s not a lot to configure. This is automatically going to perform network address translation between your WAN ports and your LAN ports. And that network address translation is all configured automatically. You simply need to plug in the connections, power up the router, and you’ll have connectivity to the internet.

Many SOHO routers also include wireless access point functionality, along with the switching, and the routing that it’s already doing. And of course, you can configure many aspects of that wireless configuration. One of those is that you can configure which frequencies you’d like to use. You can, of course, configure which bands you’d like to communicate on, whether it’s 2.4 GHz and/or 5 GHz.

You can also define the SSID name you’d like to use. This would be the name of the wireless network that appears in the list of available networks when you connect. You get to choose the security mode over the wireless network, which is how the data will be protected as it goes through the air. Normally, the WPA2 encryption is a good choice. And many wireless routers allow you to set a shared key that everyone will use, or you can configure an enterprise configuration where every user will put in their own user name and password to gain access to the wireless network.

And finally, you can decide what channel or set of channels you would like to use for this particular access point to provide that connectivity for your wireless devices. Both the wide area network connection and your local area connections on that SOHO router need to have IP addresses assigned to them. When you first connect the wide area network connection, you’ll usually get the IP address assigned automatically through DHCP directly from your internet service provider. Some service providers also require that you add authentication into the router’s configuration before it’s able to be used on the network.

For the inside of the network, the SOHO router is usually a DHCP server itself. So you’ll simply plug in any device into the SOHO router, and it will automatically get an internal IP address. These IP addresses are defined on the SOHO router itself.

My internal studio addresses, for example, have a 10.1.10.0 network. You can see the dot one is my gateway address, then I have a DHCP range that starts at dot two and ends at dot 50. So anytime I plug in a device to my network, my SOHO router’s automatically going to sign an IP address from that available pool.

DNS servers are also important to have in your configuration. These are passed to the clients during the DHCP process. If you leave these blank on my router, it uses the same DNS configuration that’s on the wide area network connection. If you have your own internal DNS servers or you would like to use other DNS configurations, you can add them into the configuration here.

If you’re plugging a wired Ethernet device into the back of your SOHO router, it’s probably set to auto-negotiate its speed and duplex. But of course, you can configure those manually on the devices that you’re connecting. Usually, it’s going to automatically define what speed you’ll be using, whether it’s 10, 100, or 1000 megabits per second, and it will decide what duplex it needs to configure– either half duplex or preferably full duplex.

If you’re connecting a device over the wireless network, then, obviously, you’ll need to enable or disable that wireless adapter. And then usually your wireless network needs to be selected from a list. And you’ll need to provide a password to gain access.

Different operating systems have different ways to set these configurations, but the names of these different options should be similar across different operating systems. For example, in Mac OS, you can see there’s an option to configure IP version 4, either automatically using DHCP, or you have an option to choose manual. And then you can add the IP addresses into your configuration by hand. The easiest configuration though, is to use DHCP– so the IP address, subnet mask router, and DNS information will all be populated on my device from the configurations that we’ve made on our SOHO router.

One set of devices that has become rather important in our small offices and home offices are the IoT devices. These are the Internet of Things devices. These are usually focused around home automation, and they’re usually connecting to your network using 802.11 wireless connectivity.

These would be your thermostats, your light switches, security cameras, door locks, and anything else that talks out to the internet so that you can gain access to these devices using your mobile phone. From a configuration perspective on your SOHO router, there’s not much that needs to be done. These devices will automatically communicate outbound, which makes it very easy for you then to connect to a central server to gain access to these Internet of Things devices.

Configuring a SOHO Firewall (10:04)

There are many options available when configuring a small office or home office router. And in this video, we’ll go through some of the more common configuration settings.

Inside of your SOHO router is a very capable firewall. It allows you to have access to the internet. But it prevents anyone from the internet from accessing any resources on your internal network. This is not generally a feature you can disable. If you’re using a SOHO router then you’re using this firewall.

The firewall in some SOHO routers allows you to configure an IP address that’s on your internal network or configure a physical port on your router to be the DMZ. This stands for demilitarized zone. This military term is the midpoint between two sides. So this would allow people to access a device that would not allow them access to the internal network. But they would still be able to access those resources from the internet.

On my SOHO router there’s an option to configure a default DMZ server. And then you can add the IP address of the device that would have access from the internet. On most SOHO routers there’s no additional configuration that’s needed. If you’re enabling the DMZ function, you’re effectively opening up that device to the internet. And that may not be the security feature you need. What you may want to do is configure specific port forwarding rules that we’ll talk about later in this video.

Worldwide, there are over $20 billion devices that are connected to the internet. And this number is constantly growing. IPv4 supports a total of just over 4 billion addresses. You can see that we have many more devices connected to the internet than we have IP addresses. As you can imagine, the address space for IPv4 is completely exhausted. We don’t have any additional IP addresses that we can assign to individuals.

The way that we’re able to get these 20 billion devices communicating on a network that can only support just over 4 billion devices is a technology called Network Address Translation, or NAT. And this is an always-on functionality that’s configured inside of your SOHO router. There are many different implementations of NAT. We’ll look at a couple of uses of Network Address Translation in this video.

The Network Address Translation functionality that is always on inside of our SOHO routers can be called Source Network Address Translation. You might also hear it called PAT, for Port Address Translation. This functionality translates all of your internal IP addresses to appear as one single IP address on the internet. This means that you’re able to have tens, hundreds, or even thousands of devices on your internal network. But to the internet it all looks like one device.

Your devices internally don’t have to do anything to take advantage of this NAT. For example, at this device, at 192.168.3.22 we’re communicating out to the internet. When it hit your SOHO router, that router would translate your internal address to look like an external address, such as 66.20.1.12. And any device that receives this traffic on the internet sees the source IP address as this external NATed address instead of your internal IP address.

This network address translation works great if you’re sending traffic out to the internet. But what if you’d like to create a service on the inside of your network and perform a network address translation in the other direction? We call this type of Network Address Translation port forwarding. This allows you to configure your SOHO router so an internal device is now available externally.

Here’s a port forwarding rule that I have configured in my SOHO router. This is my security role. And if any device accesses my external IP address over ports 8088, it will translate those ports to port 80 on the inside and send that traffic to 10.1.10.221.

You might also hear port forwarding referred to as Destination NAT, or static NAT, because we’re changing the destination IP address for this inbound traffic. This is a rule that, once it’s set up, doesn’t expire and it doesn’t time out. Anyone who accesses that port number and IP address from the outside will always have access to that particular server on the inside of my network.

Here’s an example of port forwarding. We have our internal network on the left side. And our Network Address Translation is being done by our SOHO router. We also have devices out here on the internet. There’s a 64.223.53.7 who needs to communicate to one of my internal servers. So I’ve configured a port forwarding rule that says if any traffic is inbound to 66.20.1.14, translate that destination to 192.168.3.22, which would be my server.

That means if a device on the internet sends traffic inbound to my SOHO router, when it hits my router it will look at the configuration and see the Destination NAT conversion table, or the port forwarding table, that I’ve configured inside of that SOHO router. The router then changes the destination IP address. And that traffic makes its way to my internal server.

Many SOHO routers allow you to make dynamic configuration changes using UPnP. This is Universal Plug and Play. This means that other devices on your network can automatically configure your SOHO router and make changes to the configuration at any time.

We sometimes refer to this as zero configuration. This means that instead of you manually creating port forwarding rules, you can have applications communicate directly to your router to enable or disable the access for certain port numbers. There’s no additional configurations or approvals needed for this. Those changes are simply sent to the router. And those firewall updates are made in real time.

One advantage to using UPnP is that these ports are only open when you’re using that particular application. And when you close the application those particular ports are disabled on the router. But this could also be a security concern, since you don’t have any direct control as to when certain ports are open and when certain ports are not open. And in those cases, a best practice might be to disable the Universal Plug and Play feature and have all of your configurations done manually through port forwarding.

Many SOHO routers allow you to perform content filtering inside of the router. So any communication out to the internet can be filtered by URL or can be filtered by a name that’s in that URL.

There are two common philosophies when configuring content filtering. One of these is to enable whitelisting. This means that no traffic is allowed through the firewall unless you specifically add the sites that are allowed. The other philosophy would be to blacklist traffic. That means that all traffic would be allowed through the firewall except for specific blocked sites, URLs, domain names, and IP addresses that are configured in the firewall.

Every device that connects to your network has a unique address called the Media Access Control address, or the MAC address. This allows you to configure your firewall to allow or disallow access for particular MAC addresses on your network. This is a common filtering technique that allows your network administrator to control exactly what devices are able to communicate through your router.

There’s obviously additional administration that’s required for this, because the administrator would have to add all of the MAC addresses that are allowed through your particular router. And although this can be used to limit some devices, all MAC addresses are viewable by capturing packets that may be going across your network. So as a security technique, this is not a very good way to prevent someone from gaining access to your network.

MAC addresses can be easily spoofed, which means someone can change a MAC address to get through the filter that’s in your router. Because this process of circumventing a MAC filter is obvious if you know how to do it, we don’t consider this a security technique. Instead this is called security through obscurity, which in reality is no security at all.

If your SOHO router includes wireless connectivity, then you’ll want to configure the wireless settings to have the highest possible encryption. That way, any traffic sent over the wireless network would be completely protected. On most modern routers you’ll want to configure WPA2 encryption, which is an AES type of encryption. You may also see options for WPA. But you’ll want to choose WPA2 for the best possible encryption.

Older wireless routers might even give you the option for WEP, Wired Equivalent Privacy. This is an older encryption mechanism that has a number of vulnerabilities. So you want to be sure not to use WEP on any of your devices. If you have more than one wireless access point, you may want to check and make sure that it’s using the highest level of encryption. You don’t want to use WEP or WPA. You want to make sure all of your devices are using WPA2.

And if you’re in an area with a number of different wireless access points, you may want to check the frequency settings and make sure it’s not conflicting with other devices in your area. Some devices allow you to specify the channel manually or to configure an automatic function, where the router finds the best possible frequencies for your area.

Not all SOHO routers support Quality of Service configurations. But those that do give you a lot of control over what applications are prioritized on your network. For example, if you have Voice over IP communication on your network you may want to prioritize voice communication as the highest priority and all other applications as lower priorities.

Many QoS configurations allow you to set priorities based on the type of application, the port numbers in use, IP addresses, and other settings. But you’ll want to be very careful when making these QoS settings. It can be very easy to choose the incorrect application. And you end up slowing down the applications that really need the highest priority.

2.4 – Wireless Networks

802.11 Wireless Standards (6:01)

There are a number of different standards associated with 802.11 networking. These standards are maintained by the IEEE LAN/MAN Standards Committee for the IEEE 802, and this is specifically the 802.11 standard. There have been many updates to 802.11 over time. New standards and changes are happening all the time. You can check the IEEE’s website to find out what the latest innovations are around 802.11.

If you ever see a device that says its 802.11 compliant, then it's had to go through interoperability testing. There's a Wi-Fi trademark on the box that shows that the device has gone through testing, and should interoperate with all other devices that have gone through the same testing. 802.11a a is the first of these 802.11 standards that was introduced. It was made available in October of 1999. It's a standard that operates in the 5 gigahertz frequency range, and it operates at 54 megabits-per-second.

Because 802.11a and 802.11b came out at exactly the same time, there are a lot of comparisons as to how these two standards operated. 802.11a, because it operated at 5 GHz, had a little bit smaller of a range than 802.11b. These higher frequencies are absorbed by objects that are around them. So in a normal environment, you could see about a third the range with 802.11a compared to other 2.4 gigahertz frequencies, like 802.11b or 802.11g.

Since 802.11a was one of the very first standards, it's one that has also been updated through the years, so you don't often see 802.11a devices being used any longer. The 802.11b standard was introduced at exactly the same time as the 802.11a. And unlike 802.11a, 802.11b operates in the 2.4 gigahertz range and has a maximum theoretical throughput of 11 megabits-per-second. You can see this is quite different than 802.11a that had higher frequencies but operated at 54 megabits-per-second.

Although 802.11b was a bit slower, the tradeoff was that it used the 2.4 gigahertz frequencies that tended to have a longer range than 802.11a. One of the challenges with engineering an 802.11b network, though, was other devices were also using these frequencies. Devices such as baby monitors, cordless phones, microwave ovens, and other devices used exactly the same frequencies that needed to be used by 802.11b.

In June 2003, we got an update to 802.11b. This was the 802.11g standard. This also operated in the 2.4 gigahertz range, and very similar to 802.11a, we had an increase in speed up to 54 megabits-per-second. This 802.11g standard was designed to be an upgrade and to be backwards-compatible with 802.11b, but it had the same 2.4 gigahertz frequency conflicts that we saw with the 802.11b standard.

In October of 2009, we saw an update to 802.11a, b, and g with the standard 802.11n. This was a standard that allowed connectivity at 2.4 gigahertz range frequencies or 5 gigahertz range frequencies. And we were able to get throughputs with 802.11n up to a theoretical maximum of 600 megabits-per-second. One of the ways we were able to get these larger bandwidths was through a technology called multiple-input multiple-output, or MIMO. We're able to send many streams of traffic across the same frequencies to increase the total amount of throughput on an 802.11n network.

One of the latest versions of wireless technology is the 802.11ac standard. This was an update to 802.11n and it added a number of additional features and additional throughput. This operates in the 5 gigahertz band exclusively. There are no 2.4 gigahertz options for 802.11ac. The 5 gigahertz range has a much larger set of available frequencies, so we're able to bond channels together and get higher throughputs from 802.11ac. 802.11ac was also made faster by changing the modulation. We're now able to send more data in the same amount of time.

And there were also improvements over the multiple-input multiple-output technologies we saw with 802.11n. 802.11ac introduced multi-user MIMO, so you could have eight separate MIMO streams going to multiple devices on the network, all at the same time.

Here's a summary of these five wireless standards. 802.11a operates at 5 gigahertz frequencies. It did not support multiple-input multiple-output streams, and had a maximum theoretical throughput of 54 megabits-per-second. 802.11b operates at 2.4 gigahertz, has a maximum theoretical throughput of 11 megabits-per-second. 802.11g upgraded 802.11b, so it also ran at 2.4 gigahertz frequencies, and has a maximum theoretical throughput of 54 megabits-per-second.

802.11n can support 5 gigahertz and 2.4 gigahertz frequencies, and with the addition of four MIMO streams, you're able to extend the 150-megabit throughput on a single channel, up to 600 megabits-per-second total. And 802.11ac operates in the 5 gigahertz frequency range, supports a maximum of eight multi-user MIMO streams, which means our total maximum theoretical throughput for 802.11ac is almost 7 gigabits-per-second

Wireless Network Technologies (7:16)

````````````````````````````````

When we talk about 802.11 technologies, we often talk about frequency use. And there are two major bands that we use for these frequencies. One of these bands is the 2.4 gigahertz range, and the other is the 5 gigahertz range. And there are some 802.11 standards, like 802.11n, that can use both of these ranges at the same time.

You may notice, in your configuration of 802.11 wireless access points, that you’re able to choose a channel of frequencies to use. This is a grouping of frequencies the IEEE has put together and has assigned numbers to it. For example, if you were choosing a 20 megahertz block of frequencies in the 2.4 gigahertz range that centered around 2412 megahertz, the IEEE calls that channel 1.

Some of these channels overlap with each other. So you may find in the 2.4 gigahertz range, that channel 1 and channel 2 slightly overlap. And we often say that we would like to use channel 1, channel 6, or channel 11 because we know those 20 megahertz bandwidths will not overlap with each other if you choose those channels.

Some wireless standards will use a 20 megahertz block of frequencies to be able to communicate. Others will expand that bandwidth into 40, 80, and 160 megahertz blocks. The modulation used for these 802.11 standards tends to dictate how much bandwidth will be used. For example, 802.11a, 802.11b, and 802.11g used about a 20 megahertz channel bandwidth.

With 802.11n, you have the choice between a 20 megahertz bandwidth, or you could double that to use a 40 megahertz bandwidth which was two contiguous 20 megahertz bonded channels. There’s limited bandwidth available at 2.4 gigahertz, so by bonding together and creating a 40 megahertz channel, using most of the available bandwidth.

With 802.11ac, you’re running in the 5 gigahertz frequency range which gives you much more bandwidth available. If you’re running 802.11n stations on this 802.11ac network, then you can use the 40 megahertz bandwidths that were available with 802.11n. If you’re using 802.11ac networking, then you’re using 80 megahertz bandwidths by default, and you have the option to use 160 megahertz bandwidths.

Lets visually see what this looks like for the 2.4 gigahertz range and the 5 gigahertz range. All of the colors that we see here that our blue, gold, and green are channels that are available to use in these frequencies. If you see the red color, that means that those frequencies are not available for 802.11 networking.

You can see for 2.4 gigahertz, we have three 20 megahertz blocks available- channels 1, channel 6, and channel 11, and that’s the only spectrum available in the 2.4 gigahertz range. Now, let’s look at how much bandwidth is available at the 5 gigahertz range, and you can see it’s a significant difference than running at 2.4 gigahertz. Remember that anything that’s colored red is unavailable, but all of the other colors are available as 20 megahertz channels in the 802.11 5 gigahertz range.

We mentioned earlier that 802.11n could use 40 megahertz ranges, and you can see those ranges are broken out. And, of course, anything that’s red is unavailable. If you’re using, 802.11ac then you’d be using 80 megahertz ranges. You can see there are 1, 2, 3, 4, 5, 6 of those ranges available. And if you’re using the optional 160 megahertz range with 802.11ac, you have two contiguous ranges that you can use in the 5 gigahertz band.

Bluetooth
---------

Another common networking technology we use wirelessly over a short distance is Bluetooth. This is called a Personal Area Network or a PAN, and we commonly see Bluetooth use to connect many different kinds of devices- our smartphones and tablets, our automobiles, our health monitors and smartwatches, and we also use Bluetooth for tethering and file transfers between our devices.

A popular wireless technology that we find in access badges, in our animal identification technologies, or really anything that we might need to be tracked is RFID. That stands for Radio Frequency Identification. These are very small tags that we can put in anything that we’d like to track. Here’s a size comparison of an RFID tag and a grain of rice. You can see they’re very small, so you can put them almost anywhere.

Here’s another RFID tag. This one is flat so it makes it very easy to put into things like cards that we would use for access. These RFID tags work using radar technology.
````````````````````````````````

This RF energy is set out, captured by the tag, and is used to power the RFID tag. The tag then sends out an ID signal which then can be captured. You might also find RFID tags that are already powered. Those are active RFID tags

An advanced form of RFID is one that we put into many of our mobile phones. This is Near Field Communication or NFC. This allows us to use our phones as identification devices so we're able to pay for systems with a credit card or an online wallet. We can use NFC to help with the pairing process with Bluetooth, or it can act as an identity card to prove that you are who you say you are or give you access to a locked room.

There are two major wireless standards associated with Internet of Things technologies, and one that is an open standard is Zigbee. This is an open standard called the IEEE 802.15.4 Personal Area Network. Instead of using Wi-Fi or Bluetooth, you can use a Zigbee-connected device. It uses less energy and less power than Wi-Fi and can go longer distances than a Bluetooth connection.

Unlike 802.11, which has a central access point, and all devices have to be able to communicate to that access point, Zigbee is a meshed network. This means that your Zigbee network can be quite large because all of the Zigbee devices can communicate through each other to expand the size of the network. Zigbee communicates over the ISM ban. That's the Industrial, Scientific and Medical band, and it communicates over 900 megahertz and 2.4 gigahertz frequencies in the United States.

The other competing technology for this wireless Internet of Things meshed network is Z-Wave. This is a proprietary networking type, but it is also commonly used as the Internet of Things networks for your lights, your garage door, and other home automation. Similar to Zigbee, Z-Wave is a meshed network which means that nodes can hop through other nodes on their way to the destination. This is also using the ISM band, and it's using the 900 megahertz frequencies of the ISM band in the United States.

Cellular Network Technologies (2:33)

You often hear our mobile devices described as cell phones. That's because we broke up the geography into these separate cells of communication, and we placed antennas at the corners of these cells so that we could communicate using these mobile devices. We began this method of communication with 2G networks. And we separated 2G networks into two different camps of technologies. One was GSM, which is the global system for mobile communications, and the other type of standard that was commonly used was CDMA, which is Code Division Multiple Access.

These 2G networks were built with voice communication in mind. They were built so that you could make phone calls. And the idea of sending data over this network was not part of the original engineering.

There were minor changes made with 2G that could support some data exchange, but the primary focus was on voice communication. 3G networks were introduced in 1998, and these networks provided more data functionality than we had with the 2G networks. These 3G networks really changed how we started to use our mobile devices, because this increased bandwidth meant that we could have different types of applications.

We were able to run GPS technologies and have video on demand and use much more data than we were using with 2G. With 4G technology, we began to consolidate the type of wireless networking that we were doing over these mobile networks. Most of this consolidation consisted of LTE, or Long Term Evolution, networking.

This was based on GSM and EDGE, which was the enhanced data rates for GSM evolution. So we took the data that we were getting from 3G and improved what we were able to do with 4G networks. In fact, the LTE standard supported download rates of 150 megabits. And an improvement to LTE called LTE Advance doubled that to 300 megabits per second.

Of course, we're already planning for the update to 4G, which will be our 5G networks. And a roll out of those will be in late 2018, 2019, and then worldwide, we'll see rollouts in 2020. 5G technologies will be able to use much higher frequencies. And if you're using those frequencies, you could see some significant performance improvements. This will not only increase the number of frequencies available but will have some significant improvement in the data throughput as well.

2.5 – Network Services

Network Services (10:55)

Web Servers

This is a picture of a typical data center. It’s a room with many different rows of racks. And inside each of these racks are many different computers performing many different functions. In this video, we’ll look at the different devices that might be inside these racks and give you an idea of what network services you might expect to see.

One of the most popular server types on the internet is the web server. This is a web server that responds to browser requests sent from the browsers on your computer. This is using a standard set of protocols that is HTML or HTML5.

The web pages are stored on the server. So your browser on your computer will request those pages from the server, and those will be downloaded over the network to your browser. These can be either static pages that were created previously, or they might be dynamic pages that are created when the client is requesting them.

Most organizations need a central server they can use to store documents or videos or any other files that are in use by their users. These file servers will use a standard form of file management. In Windows, that’s usually SMB, or Server Message Block. If you have Mac OS, then you’re probably using Apple Filing Protocol. Of course, your users don’t know anything about SMB or AFP. They simply use the file manager available in their operating system, and the protocols between their computer and the file server handle all of these transactions.

Printer Servers

If there are printers on your network, than you probably have print servers that act as a middleman between you and that printing device. This might be software that’s running inside of a computer, and then the computer is then connected to the printer. It might be a print server like this one that plugs into the printer itself, and there is a server that runs here that acts as the middleman between you and that printer.

There are a number of different printing protocols that you might see. If you’re using Windows then you’re using SMB, or the server message block. But you could also be printing using the Internet Printing Protocol, or IPP, or the Line Printer Daemon, which is LPD.

DHCP (Dynamic Host Configuration Protocol)

If you turned on your computer and you were able to get access to the network without any additional configurations, then you’re probably using DHCP, or the Dynamic Host Configuration Protocol. This is a protocol that will automatically configure the IP addressing for your device. This is a very common service. Almost every small office or home office router has a DHCP server inside of it. And if you’re in an enterprise, you probably have multiple DCP servers that handle the DSP configurations for all of your enterprise devices.

DNS Servers

If you visited my website, you probably didn’t type in the IP address of my website into your browser. Instead, you typed in www.professormesser.com. But something needed to translate between the name of my site and the IP address that could then be used to communicate across the internet. That conversion process occurs on a DNS server, a Domain Name System server.

DNS is a very distributed system. There are thousands and thousands of DNS servers on the internet. These are obviously very critical resources. If you’re using DNS at home, you’re probably making use of a DNS server at your internet service provider. If you’re an organization that has your own internal services, then you probably have your own

DNS servers that you run in your data center.

Proxy Server

Some organizations use a proxy server for all of their internet communication. As the name implies, the proxy server is an intermediate server that sits between you and some other third party resource. For a proxy server to operate, you would bring up a browser on your computer as you normally do, and you would try to access a server that's on the internet. Instead of you accessing that server directly, you're really sending the request to the proxy server.

The proxy server then makes the actual request to that resource and receives the response from that resource. The proxy server then examines the information that it's received. And if everything looks OK, it sends that information down to your workstation. Since this proxy sits in the middle of the communication, it's a perfect place to perform some security functions. For example, it's very common to do access control, malware scanning, and content filtering on the proxy server.

We're used to reading through our email messages on our mobile devices and our computers. And the device that allows us to do that is the mail server. This is where we would store any incoming mail and be able to send any outgoing mail. The mail server is usually managed by your internet service provider or your mail provider, or you might have your own mail servers inside of your organization.

Email continues to be a very critical resource. We rely on our email 24 by 7 to provide connectivity, and you'll find that most organizations have very stringent requirements for uptime relating to their mail servers. If you've ever logged into your corporate network or connected to your VPN, then you had to put in a username, a password, and perhaps other authentication credentials.

The device that checks these credentials is an authentication server. It's a centralized repository of all of the authentication credentials for your organization. We don't usually see an authentication server on a home network. And that's usually because it's a small group of people, and you can manage your usernames and passwords individually.

But in the enterprise, you need a centralized place where you can enable or disable accounts or make global changes to configurations for individual users. These are almost always a redundant service. You don't want to lose your authentication capabilities, or no one would be able to gain access to the network. Instead, the authentication is usually spread across multiple servers. So if one server happens to go down, your system can still authenticate your users.

If you're an organization that has any number of these different services, then you probably need a SIM. A SIM is a security information and event management device. It allows you to consolidate logs from all of these different services into one single database. This is commonly used by the security team to look for real time alerts and be able to look at trends over time, but it's also consolidating logs from many different devices- your routers, your switches, your file servers, your DCP servers, and more. And you can usually perform some advanced reporting with all of this data that you've stored.

You're able to link very diverse data types and create reports over a very long period of time. Since you're storing information from so many different devices, it makes a perfect place for forensic analysis. If there's a security event or something that you need to find out more information on, you can drill down into the details and find out across all of these different services exactly what happened.

There's a standard process for transferring these types of log files to a SIM, and this standard is called syslog. This means that no matter what type of device it happens to be, as long as it can communicate its logs back through syslog, you can consolidate everything into this central database. This means also that you're going to need to store all of this data over a very long period of time, so you're probably going to need a lot of storage space.

Some syslog consolidation tools and SIMs will use WORM drive technology. That stands for Write Once Read Many. And so you're able to write once onto optical drives, and no one is able to change that information once it's been written.

IDS (Intrusion Detection System) vs IPS (Intrusion Prevention System)

Network administrators need some way to watch for intrusions onto their network. And they do this by using either an IDS or an IPS. That’s an Intrusion Detection System or an Intrusion Prevention System. These intrusions could be someone trying to take advantage of an operating system vulnerability. They might be looking to perform a buffer overflow, or they may be attacking a database with a database injection.

The IDS or IPS is looking for these types of attacks. And if any of those attacks are seen going across the network, you’re able to react to those particular events. The type of reaction that’s available is going to be based on the type of technology you’re using. If you’re using an intrusion detection system, then you’re able to see that that particular exploit was attempted.

And at that point, you can alarm or alert that that particular situation occurred. If you’re using an intrusion prevention system, you have the additional capability of blocking that particular event from occurring on the network. So if somebody did attempt a database injection, you could stop that communication on the network before it ever reached the database server.

These days, you might see many of these different components collapsed into a single device. This would be an all-in-one security appliance. You might also hear this referred to as a next-generation firewall or a Unified Threat Management device, or UTM device. This could also be called a web security gateway.

And this device might be your URL filter. It might provide some type of content inspection from your users. It can look for malware going across your network, and it could stop spam from coming into your network.

This might also be network connectivity. So it may have a wide area network CSU/DSU associated with it. And of course, it may have routing and switching technology as well. This could act as your firewall. It may include an IPS as part of its technology, and it might even be able to do bandwidth shaping and quality of service all from one single device.

Endpoint Management Server

If you’re managing a large group of devices on your network, then you know performing one single update to the operating system can be a very arduous task. You’d have to go to every single desktop, run that installation process, reboot the system, and make sure that it was working.

With an endpoint management server, you can do all of this from what we call one pane of glass– one console that allows you to do this on all of your workstations.

So you could sit in one chair and perform software installations, driver installations, update the software that’s on these systems, perform security patches, and do remote troubleshooting. Most endpoint management services require that you install an agent initially on everyone’s workstation. But once that installation is done, you’re able to manage everyone from this central console.

Legacy Systems

It’s not uncommon for many companies to have a number of legacy systems that are still running on their network. These may be systems that have been running for years in their network. But they also may be running a very important set of services, and so it’s important that we’re able to maintain and keep these systems running.

Although we talk about learning the latest and greatest operating systems and applications, it could be just as important to learn about these older systems as well. And as a technologist, you may be asked to maintain embedded systems as well. These are systems that are not the normal operating systems you might work with, but they have a connectivity to the network, and they are an electronic system. These embedded systems might be the time card clocks, or they might be the security systems for your company. And so you may be responsible for maintaining all of these embedded operating systems as well.

2.6 – Network Configurations

An Overview of IPv4 and IPv6 (5:51)

If you’re setting up a workstation to connect to the network, it’s going to need a configuration that includes IP version 4. This is the most popular networking protocol in use today so it’s important that you know all of the different configuration options for IPv4. There’s also a newer IP protocol appearing, IP version 6 or IPv6. This protocol is included with many modern operating systems so it’s also important to know how to configure IPv6, as well.

IPv4

Here’s an IPv4 address, it’s 192.168.1.131. An IPv4 will always follow the same format of four separate numbers separated with a period between each one of them. As you can see in this binary representation, this is 32-bits long or 4 different bytes long and each byte separated with that period.

Since you have 8 bits to work with, the number that can appear in each one of these sections of an IPv4 address is a number ranging between zero and 255. Because each one of these octets in an IPv4 address are 8 bits long, the values that you would see in each one of these sections is a number between zero and 255.

IPv6

IP version 6 addresses are much bigger than the 32-bit addresses from IP version 4. IP version 6 are 128-bit addresses, which means we can have a very large number of available addresses with IPv6. This means of the 6.8 billion people on Earth, we could begin assigning IP version 6 addresses. And each person could add this many IPv6 addresses for each individual.

IPv6 addresses look very different than IP version 4. You can see that they are separated into eight different sections. And each one of those is a 16-bit or 2 byte section. Instead of using periods or dots to separate the addresses as we do with IP version 4– in IP version 6, we use a colon. And the IP version 6 address is represented in hexadecimal, rather than in decimal.

So you can see, fe80000000000005d180652cffd8f52. And that is one entire IPv6 address. Fortunately, there are ways to abbreviate these IP version addresses. If there leading zeros– such as 0652– you can simply state that as 652, as an abbreviation. If there are consecutive sections of this address that have zeros, we can remove all of those zeros and replace them with a double colon. This means it will become more difficult to memorize an IPv6 address. So we’ll need to rely on our DNS servers so that we can refer to these devices by name, rather than IP address.

If we look at most IPv6 configurations, the first half or the first 64 bits of the address, are generally referred to as the network prefix. And then the last 64 bits of the address are the node or the network address of the device.

Configuring wiht IPv4

If you’re troubleshooting IP version 4 or you’re making configuration changes to IPv4 on someone’s workstation, there are a number of settings you’ll need to check. The first is the IP address. Every device needs an unique IP address. You don’t want to have duplicate IP addresses on the network. And usually, if you do assign a duplicate IP address, the operating system will warn you that another device on your subnet shares that same IP address.

Subnet Mask

The second piece of information you’ll need to configure is the subnet mask. An example subnet mask is one, like, 255.255.255.0. This is a value that’s used by the local device to determine what IP subnet it happens to be on. The subnet mask is usually something you can figure on the local workstation. It’s not a value that’s generally transmitted across the network. And if you’re someone who’s configuring an IP address on a device, it’s very common to ask at the same time for both the IP address and the subnet mask for a workstation.

Default Gateway

The third piece of information you’ll need to configure is a default gateway. This is the IP address of a router that’s on your local subnet. If you don’t configure a default gateway, your workstation won’t be able to communicate outside of its local network. And it certainly won’t be able to communicate to the internet.

Another piece of information that’s almost mandatory to configure on someone’s workstation is a domain name server IP address. When we type the name of a website in our browser, we don’t use IP addresses. We use the name of that site. We type in professormesser.com or Google.com. And we have no idea what the IP address of that device might be.

But, of course, your routers and all of the routers in between you and that web server need to know the IP address of those devices. That means there needs to be a translation between the name of the device and the IP address of the device. And to make that translation, we use a DNS server or domain name system server.

If you look at the DNS configuration for your operating system, there’s usually at least two slots available to put DNS IP addresses. And very often, there’s even more than that. For example, on my device, I have two IPv4 DNS servers listed- 8.8.8.8, which is the DNS server at Google. Google also has a second DNS server available at 8.8.4.4. And you can see I have IPv6 addresses available for IP version 6 DNS resolution.

We list multiple DNS servers in our configuration in case one of those servers becomes unavailable or we’re not able to communicate to that device. That way, we have at least a backup system that we can use to continue to perform this name resolution.

Assigning IP Addresses (7:19)

In the early days of IP, you had to manually configure everything. You would at an IP address, a subnet mask, a gateway address, the DNS servers, NTP servers, and anything else that needed configuring for your TCP/IP to work properly. All of this changed in October of 1993, and the bootstrap protocol was introduced.

We often refer to this as BOOTP. But BOOTP didn’t work for everything that we needed to have configured automatically. For example, when we added voice over IP phones to our network, there was no way for BOOTP to add voice over IP gateway information.

BOOTP also had no way to know when an IP address was suddenly available again. So we updated BOOTP into a new protocol called dynamic host configuration protocol, or DHCP. And if we are getting automatic IP addresses on our devices these days, then you’re probably using DHCP to accomplish that.

Let’s step through the process that DHCP uses to obtain an IP address. I have a simple IP subnet listed, and on this IP subnet is a switch. And on this switch, we’ve connected a client workstation, a DHCP server, and a router.

The DHCP process works on a local subnet. But on our network, we have a DHCP server on our local subnet and a DHCP server that is not on our local subnet. To be able to use this DHCP server that’s on a different IP subnet than ours, we need to configure our local router to have a DHCP relay address configured.

Sometimes, you’ll hear this referred to as an IP helper-address. This tells this router that if it ever sees any requests for DHCP, to also send them to this DHCP server that’s outside of our local subnet. This means we’re now ready for any problems that might occur. If our local DHCP server has a power supply that goes bad and is suddenly unavailable, we can still use this DHCP server that’s located elsewhere, because we’ve configured a DHCP relay.

When we first turn on our client workstation, it does not have an IP address, so it’s going to send a broadcast out to UDP port 67 over the network. This broadcast will make its way to every device on our local subnet, and it will eventually end up at the DHCP servers that have been configured on our network. Those DHCP servers will examine the request. And if they have an IP address that’s available, they will make an offer to this client workstation using a broadcast to UDP ports 68. Those broadcasts from both DHCP servers will be seen by the original client workstation.

When multiple offers are made to a device, the device usually chooses the first offer that was received. Now that it knows that an IP address is available, our client workstation can send a broadcast over UDP port 67 to request that IP address. Once the DHCP server receives the address, it can send a formal acknowledgment to that address to the client workstation over UDP port 68. And at this point, the client workstation can configure itself with that IP address.

On each of those DHCP servers, there was a pool of addresses configured. So any time a request was made for an IP address, any random set of IP addresses that was available could be sent down to that client. This means that your IP address could occasionally change. The IP address you have this week might be different than the IP address you have next week.

However system administrator may prefer that a device always has the same IP address. For example, they may want a server or a printer to always have the same IP address every day. One way to accomplish this would be to disable DHCP completely on that device. This means you have to manually configure all of the IP address settings. So you as the administrator would have to manually type in the IP address, subnet mask default gateway, DNS settings, and anything else relating to IP.

If any of these values need to be changed later you would have to revisit this device and manually reconfigure all of those settings. A much more flexible way to accomplish this will be to create an IP reservation on the DHCP server where you can associate the MAC address of this device to a specific IP address. That way if you need to make changes, you can go to your DHCP server, and those changes will be propagated to all of these devices.

If you turn on your computer, and you don’t receive a response from a DHCP server, you might still be able to communicate with other devices on your network. You’re able to do this thanks to automatic private IP addressing, or APIPA. This is what we call a link local address. It’s an automatic address that’s assigned to your workstation that allows you to communicate on your own IP subnet, but you’re not able to communicate outside of your local subnet.

There are a range of IPv4 addresses assigned just for APIPA. This ranges 169. 254.0.1 through 169.254.255.254. The first and last 256 addresses are reserved, which means if you look at the available IP addresses for workstation, they’ll fall in the range from 169.254.1.0 through 169.254.254.255. This means if you turn on a device, and you find you’re not able to communicate to the internet, and when you look at the IP addresses, they fall in this particular range, you know you’ve been assigned an APIPA address.

This process of assigning an APIPA address is done automatically by the operating system. And before it puts that address onto your workstation, it sends an Address Resolution Protocol, or ARP frame out to the network to make sure that nobody else is using the IP address that it wants to assign to your workstation. Here’s an example of the IP config information in Windows for a device that has been assigned an automatic IP address. You can even see that it says autoconfiguration IPv4 for address, and this address is 169.254.228.109, which certainly fits into that range of APIPA addresses.

This idea of having a link-local address is also available in IP version 6. And in IP version 6, it’s a functionality that’s automatically assigned to every IPv6-enabled interface. So you may find that your local IPv6 address not only has a link-local address, but it also has an IPv6 address that allows it to communicate outside of your local subnet.

The range for these link-local addresses in IPv6 begins with fe80 and then all zeros, with only one subnet allocated. Which means effectively, this is an IP address that is fe80 with the rest zeros in the first 64 bits, and then the last 64 bits are assigned as the node address. These last 64 bits that are assigned to the device are not always a random value. Often, they are converted from the MAC address of the device so that there is some uniqueness to the link-local address in IP version 6.

Using IP Addresses (6:32)

Knowledge of assigned IP addresses to your devices. There’s many ways that you could take advantage of this. In this video, we’ll look at many ways to use these IP addresses.

One common type of virtual private network, or VPN, is one that uses SSL, or Secure Sockets Layer. These SSL VPNs use a very common protocol, which is TCP/443. This is the same protocol that we use to communicate securely to web servers inside of our browser. This means we can avoid a lot of problems with firewalls by using this very common and well-used protocol.

SSL VPNs are commonly used for end user communication so that you can have a secure tunnel between your device and your corporate network. And SSL VPN can also be relatively easy to install. You would simply assign authentication credentials to a user so they would use the same username and password they always use to gain access to this SSL VPN. You don’t necessarily need to roll out digital certificates to everybody’s workstation or configure shared pass phrases like you do with IPSec.

Many SSL VPN clients can run inside of a browser, or they might already be built into your operating system. You simply provide the username and password and the IP address that you want to connect to, and you’ve got an SSL VPN tunnel. You often hear these SSL VPNs referred to as client-to-site VPNs, or remote access VPNs, because you can be anywhere remotely out in the world and be able to communicate securely back to your corporate network.

If you have your laptop at a hotel or a coffee shop and you want to communicate back to corporate, you simply start the SSL VPN software on your laptop, and it creates this encrypted tunnel back to your VPN concentrator at your corporate facility. This means if anyone was to capture any of this traffic between your workstation and this VPN concentrator, all they would see is encrypted communication.

Your VPN concentrator is responsible for then decrypting that information and sending it into the corporate network. When this information is sent back to your remote laptop, it is encrypted by the VPN concentrator and sent over that encrypted tunnel and then decrypted by your laptop. This means that no matter where you are in the world, you know you can start your SSL VPN software and have this encrypted secure tunnel back to your corporate network.

A LAN is a local area network. We define this as a group of devices that happen to share the same broadcast domain. For example, we have two switches on our network. The switch on the left and all of the devices connected to that switch are one broadcast domain. And we have a switch on the right, and there’s devices connected to that switch. Those devices are on a different broadcast domain.

We often maintain the separation between different local area networks for security reasons and to maintain the efficiency of the network. But this also means that we would have to have a separate switch every time we wanted to have a separate broadcast domain. To simplify this, we create a virtual local area network or a VLAN, which means that we can have a single switch. But inside the switch, we are logically separating these different networks into two pieces.

We still have the red network on the left, and all of the devices on the red network can only see the other devices on the red network. And then we have the blue broadcast domain network on the right side. And again, only the blue devices can communicate back and forth to other blue devices. This greatly simplifies the administration and the cost of having multiple switches on our network. Instead, we can configure a single switch to act and operate as if it’s multiple switches.

For example, here’s a single switch where three separate VLANs have been configured. We have the red VLAN, which is VLAN 1. That’s for the gate room. We have VLAN 2. That’s the blue one that has the dialing room. And then the green VLAN is VLAN 3 for the infirmary.

So all of the devices that are connected to the red ports can communicate to each other on VLAN 1. The devices on the blue network can communicate to each other and the devices on the green network can communicate to each other. And none of the devices on these separate networks are able to communicate across that VLAN separation. That allows you to maintain the security and the efficiency of the network while minimizing the number of switches that you need to have running at any particular time.

It’s estimated that there are over 20 billion devices connected to the internet. But we know that IP version 4 can only support just over 4 billion addresses. This also means that the entire address space for IPv4 has been easily exhausted at this point. But we still have a requirement to connect these 20 billion devices that are on the internet.

The way we do that is by using Network Address Translation, or NAT. This is just one of the ways that we can take advantage of using NAT. But it’s one of the most common ways so that you can have many devices on the inside of your network all translating out to a single device on the public internet side.

Network Address Translation literally changes, or translates, one IP address to another. For example, we have an internal network, where Vala has her laptop. And she wants to communicate out on the public internet to my website, professormesser.com. When she sends traffic from her workstation, the source IP will be that of her laptop, which is 10.10.20.50. And she wants to communicate to my web server, which is 104.20.19.63.

When she sends this information to her router, her router has been configured to perform Network Address Translation. And it changes the source IP from her internal address to the external address on the public internet and then sends that information to my web server. When my web server wants to respond back, it simply reverses those IP addresses, has the source IP as my web server, and the destination IP as the public IP address on the internet. When it’s received by that router, the router translates it again back to Vala’s internal IP address and sends that information down to her laptop.

This Network Address Translation happens for all of the devices on your internal network. So you can have hundreds or even thousands of devices on your internal network all being translated to one single IP address on the internet.

2.7 – Internet Connections

Internet Connection Types (9:11)

There are many different ways to connect your home and your business to the internet and in this video we’ll look at a number of these internet connection types. A very common internet connection type in the home is a cable modem. We sometimes refer to this as broadband communication because we are sending information over many different frequencies on the same wire. This also can be different traffic types on these different frequencies, so it’s not uncommon to have video, voice, and your data coming across this single cable modem connection.

You may sometimes hear this cable modem connection referred to as DOCSIS, which is data over cable service interface specification. This is the standard that is used on cable networks to send data across to these cable modems. This is what we consider high-speed networking. These cable networks can go very high speeds. Very commonly you’ll find four to 250 megabits per second, but you can get up to gigabit speeds running on these cable modem connections.

The cable company isn’t the only one providing internet connectivity. Very commonly your local telephone company is providing connectivity through DSL connections. This is technically ADSL, for asymmetric digital subscriber line. This uses your existing telephone lines, which makes it very easy to simply add a modem into your home and you’re connected to the internet. One of the challenges you have with DSL is that you have to be somewhat close to a central office or a CO.

The download speed that you’re going to have will be directly proportional to how far away you are from that central office and the limitation is somewhere around 10,000 feet, which is not an incredibly long distance when you consider how dispersed are different homes are away from these central offices. You'll generally get 52 megabits per second down and 16 megabits per second upstream, but these numbers can vary widely depending on how far away you are from the CO. As you begin to move farther away from the CO, you'll start to see these speeds get slower and slower.

Another type of internet connectivity we don't see much any longer are dial-up connections. These are using our existing analog voice telephone lines and sending data communication over that connection. You'll commonly see 56 kilobits per second modems. This is significantly slower than a DSL connection or a cable modem connection, although you can't compress the data bit to get speeds up to 320 kilobits per second. Obviously, when you compare this relative to cable modem or DSL, these speeds are relatively slow, which makes using a dial-up connection difficult to scale, especially if you need to connect many different people to the internet.

Although you no longer tend to find a dial-up connection at home, it's very common to use them in large enterprise environments. If you lose the connection to a remote site over a cable connection or a DSL, you might be using these traditional analog dial up modems to provide some connectivity back to those sites.

We've been using fiber in the enterprise for many years to provide internet connectivity, and we're starting to see more fiber rolled out to the home. This provides very high-speed networking and allows us to send many different services over that single fiber. So voice connectivity, our video connections, and our data can all be running over a single fiber to our house.

This increase in available bandwidth also brings a number of new services. You have a lot more HD channel connectivity than you might have with a copper-connected service. And this also allows you to send and transfer a lot of different types of data out to the cloud. You might also see enhanced capabilities with DVR and video capabilities using this additional bandwidth.

Our internet connectivity doesn't have to be limited to connectivity on earth. We can sometimes connect to the internet using satellites that are in space. This satellite networking allows us to communicate directly to a satellite, which then sends that data to a station down on earth and then reverses that to get the data back to us. This has, as you might expect, a relatively high cost compared to traditional terrestrial networking such as cable modem or DSL connectivity, but your speeds are pretty good. You get around 50 megabits per second down, three megabits per second upstream are common to find with satellite networking, but this does allow you to connect to sites that may not have the ability to connect to a cable modem or DSL connection and you're able to be in a remote site or somewhere far away from the central office and still have relatively high-speed internet connectivity.

There are a number of challenges with satellite networking. One of these is that you have a relatively high latency. It does take time to get that data up to a satellite and then back down to earth. So if you have an application that requires a very low amount of latency, this may not be the type of connectivity you'd like. Those of you that have satellite connections for your television at home know that the other problem with this type of connectivity is when it rains. If you have a very heavy thunderstorm, that rain coming down can block this two gigahertz signal from going from your dish out to that satellite connection. So while this storm is going on outside, you won't have any type of Internet connectivity.

An older style of internet connectivity, which still has some limited functionality in today's markets, is ISDN. It stands for integrated services digital network. There are two different types of ISDN you might find. One is what we call an ISDN basic rate interface, or BRI. You'll sometimes hear this referred to as a 2B+D. This was referring to the two bearer channels, which are actually sending data over these ISDN connections, and the single signaling channel, or D, channel.

These two bearer channels are 64 kilobits. So we're not talking about high-speed connectivity that you might have with cable modem or DSL, but this is certainly better than using a dial-up connection. The signaling channel, or D channel, which is a 16 kilobit per second channel when you're working with BRI is managing all of the communication over this connection. So it sets up the connection, it tears down the connection, and sends any management information while the call is going on.

A larger scale ISDN is the primary rate interface ISDN, or a PRI. This is usually delivered over a T1 or E1 connection depending on what country you’re in. And a T1 connection supports 23 bearer channels and a signaling channel. And E1 supports 30 bear channels, a signaling channel, and a separate alarm channel.

Although you could certainly use these very large bearer channels to send internet connectivity over a PRI, it’s also common to see PRI used as voice channels that are coming from your public switched telephone network, that’s your local telephone company, and connecting to a private branch exchange or a local phone system inside of your company. If you’re not converting over to voice over IP, you may be using some of these legacy ISDN connections to provide all of your voice communication.

Modern cellular networks allow us to have internet connectivity from practically anywhere. We now have a mobile phone that allows us to have both voice and data access simultaneously. These cellular networks have many different antennas set up in a geographical area where the land is separated into cells. That’s where the idea of a cellular network comes from. And our mobile devices use these antennas to be able to communicate back and forth to the internet.

Not only do our mobile phones have internet connectivity, but we can connect a wire from a laptop to our mobile phone and provide the laptop with the internet connectivity as well. That’s called tethering. And if you’re connecting many devices to your mobile phone over 802.11 wireless connectivity, you’re effectively turning your phone into a mobile hotspot. This way anyone in your local area is able to use your internet connectivity on your phone to provide internet access for all of your devices.

In your metropolitan area, you may have the option of a line-of-sight internet service. This is a wireless internet service that’s able to provide access over a very wide geographical area. This is a line-of-sight communication, so there’s usually antennas placed very high that are able to communicate to many different homes simultaneously in one geographical area. There are also options for non-line-of-sight, this would usually be slower speeds using lower frequencies. And a very common type of line-of-sight service is WiMAX. This is the worldwide interoperability for microwave access. This provides wireless high-speed internet connectivity by simply putting an antenna outside of your house and accessing those WiMAX antennas in your area.

Network Types (4:51)

Is your network connecting to devices that are in the same room as you? Or are they connecting across the country or across the world? In this video, we’ll look at the many different network types.

If you’re connecting devices together in your immediate geography, then you’re probably using a Local Area Network, or a LAN. A LAN is usually connecting devices in the same room or perhaps on the same campus. There may be a number of different buildings that are close by. And you’re able to connect them over higher-speed ethernet connectivity. This gigabit and even 802.11 wireless connectivity could be considered a Local Area Network.

Once you go to slower speeds than this, you’re probably not connecting to anywhere that’s in your local area. For example, if you’re connecting to another city or another country, then you’re probably using a Wide Area Network, or a WAN. This is connecting one Local Area Network at one location to another Local Area Network that is somewhere very far away, geographically speaking.

There are many different ways to connect over a Wide Area Network. You could be using point-to-point serial connections, or MPLS connections. It’s common to have those type of connections be a fiber or a copper that’s in the ground and going from your location in the ground to another location somewhere else.

This could, of course, be using non-terrestrial communication. It’s common to have wide area connections using satellites, where you send all of your data to a satellite. And it communicates back down to a ground station and then reverses that process to get back to you.

If you’re using a network that is in your immediate area then it’s probably a PAN, or a Personal Area Network. If you’re using Bluetooth or infrared connectivity, or you’re paying for something with your mobile phone using a Near Field Communication– or NFC–

connection, you can consider all of those Personal Area Networks.

For example, if you get into your car and connect your phone to your car over a Bluetooth connection, that is certainly a very popular Personal Area Network. We often have these wireless headsets that we put in our ear. That’s also using Bluetooth. So that would be considered a Personal Area Network. And if you’re working out on a treadmill or an elliptical and sending that telemetry back to your mobile device, that’s also using a Personal Area Network.

We mentioned earlier that you can have a Local Area Network that is in your campus. You can also have a Wide Area Network, where you are communicating to another city or another country. But there’s also a middle point where you’re communicating within the same metropolitan area. We call these MANs, or Metropolitan Area Networks. These are usually managed by one central network provider that’s in your area, which makes it very easy for them to connect up one remote site to another remote site that may be on the other side of the city.

There used to be many different ways to set up connectivity over a Metropolitan Area Network. But these days, your local network provider is going to hand off an ethernet connection. And you’re simply going to plug into an ethernet port on your local equipment. It’s also common to see Metropolitan Area Networks run by a local government. Since these local governments already own the right of way, it becomes relatively easy for them to put conduit in the ground and put fiber between different locations within a single metropolitan area.

One relatively new type of networking, especially networking in our home, is a WMN, or a Wireless Mesh Network. These are usually associated with the Internet of Things. You can think of having all of these different devices inside of your home, being able to create an entire cloud of devices communicating and hopping between each other to complete the entire network.

There can be many different devices, all able to self-form together to create these wireless mesh networks. So you may have installed the latest garage door opener, front door lock, and lights in your home. And all of these wireless devices can now form a Wireless Mesh Network. Because all of these devices are communicating to multiple devices in your network, they’re also able to self-heal. So if one of your devices happens to go offline, there’s still many other ways that it can use to communicate to all the other devices in your network.

You’ll find a few different types of WMN networks in your home. There’s certainly 802.11, which has many new technologies coming out for mesh networking. There’s also Zigbee and Z-Wave networking technologies. So depending on the type of Internet of Things devices you’re using, you may be using one or more of these devices to provide this mesh network.

2.8 – Network Tools

Network Tools (10:46)

As a network administrator, you’ll be asked to troubleshoot a number of different network issues. So you need to be sure you have the right network tools in your tool bag.

If you’re building your own cables, then you’ll need a cable crimper. This is the device that pinches the modular connector onto the end of the cable. This cable crimper, for instance, has two different connectors on the end, one that is a six-position, which is for RJ11. And one is an eight-position, which is used for crimping RJ45.

This is usually the last step of the process. You’ve run a cable from someone’s desk. You’ve run it up the ceiling. It’s gone all the way down into a network closet. And now you need to put a connector on the end of that cable. You’ll put the modular ethernet connector on and use the crimper to fasten it to that connection. The crimper’s job is to take the copper that’s inside of that modular connector and push it through the insulation of that wire, so that you have copper-to-copper connectivity going from the wire itself into the connector and ultimately into your network device.

Let’s look at a modular connector that has not been crimped onto a wire. Before you use the crimper, you’ll notice the copper connections are sticking out just a little bit. When you finally perform the crimp it will push down all of those copper connections.

And you’ll notice, they have these pointy tines at the end of the connectors. Those are the connections that are going through the insulation of the wire and making contact with the copper that’s inside of those wires. Once you make the crimp, you’ll notice that the copper connectors are now down inside of the connector itself. And notice that those pointy connections at the end have now been pushed into the wire itself to make that copper connection.

You’ll also notice that the crimper pushes in a piece of plastic at the bottom that holds the cable in place. That way, once you’ve made this good crimp there’s no way for that wire to accidentally pull out of the connector.

If you’re going to be troubleshooting or working with these copper connections, you’re going to want a good pair of crimpers. You might also want a good pair of cable snips. These are also called electrician scissors. And optionally, you might also want a good wire stripper, especially if you’re working with different kinds of wiring and need a quick way to strip away coax or other types of wired connections.

You also want to be sure that the modular connectors that you’re using match the type of cable you’re connecting to. Category 6A cabling will require connectors that are designed for category 6A. So make sure that the crimper and the connectors you’re using all match the wiring that you’re running on your network.

Performing the actual crimping process is a bit outside the scope of the Network+ exam. But if you do start building out your own cables, it may seem a bit difficult at first to work with these very small wires, get them in the right order and into the modular connector. But after some practice and a number of times of crimping down the wires in the wrong order, you start to get the hang of it. And it becomes a lot more easy to troubleshoot and to replace these copper connectors on these modular ethernet runs.

Another incredibly useful tool to have in your tool box is a multimeter. This can provide voltage and continuity settings. For example, you can plug into a power source that’s providing AC power and measure exactly how many volts of AC power is coming from that connection. It’s a good way to check to see if a particular power source is either working or not working, or may be providing a different amount of voltage than what you were expecting.

The “multi” in multimeter means that it does more than one thing. You’ve got a number of different voltages and settings that you can check for. And of course, you can check for DC voltage as well. So if you’d like to check the voltage coming from a laptop power supply or PC power supply, or you’d like to see how many volts are available in a battery, the multimeter is a great tool to use.

These multimeters are also great for performing continuity tests. So you can check a fuse to see if the fuse is still working. Or you can check pins on both sides of a wire to see what pins on one side are connecting to which pins on the other side. This allows you to build a wire map to determine the type of wiring you might be working with.

If you have more than a couple of wires in your environment, then you’ll want to invest in a tone generator. This allows you to follow or track where a wire is going from one end to the other by simply following a tone. This is usually two different components. One is the tone generator itself. You plug this into the wire. And it places an analog sound onto that wire.

The other piece of this tone generator is the probe. This is an inductive probe, which means it doesn’t have to physically touch the copper to be able to listen in to that audio that’s being placed by the tone generator. You just need to get close. And there’s a small speaker that is on the inductive probe that allows you to listen in to see if you can hear that tone coming through a cable.

This means you could have a bundle of hundreds of cables and still be able to trace exactly what cable you’re looking for in that bundle. You simply connect the tone generator to the wire. This tone generator can connect to many different types of connections. It could be coax or RJ11 or RJ45. And then you use your inductive probe to find the sound that’s coming through the wire.

Here’s four ethernet cables that are on my network. And I put a tone generator on the other end of one of these cables. But I don’t know which one of these it happens to be. This, of course, could be a bundle of 100 cables. But the process is exactly the same.

I take my inductive probe, which has a button on the front that I hold, and I simply touch the inductive probe to the different cables. You’ll notice, you don’t hear anything. You don’t see anything. But when you finally get to the cable that does have the tone generator on the other end you’ll hear the sound. You’ll see the light flashing. And you know that this must be the cable that has that tone generator on the other side.

Now that we know where the two ends of this wire happen to be, we may want to connect a cable tester to those two ends of the wire and perform some simple continuity tests. A cable tester is going to be able to tell us if all of the pins are connecting– from pin one to pin one on the other side, pin two to pin two, and so on. If there any missing pins or crossed wires, it may identify those as well.

The cable tester tells us if we’ve wired things properly. But it doesn’t tell us the quality of the wiring. If we need to perform cross-talk analysis or frequency tests then we may want to use a time domain reflectometer, which is, of course, a much more advanced function than something like a cable tester.

Your tool box may also include a number of loopback plugs. These are used to send traffic going out of a particular interface, loop them around, and send them back into that same interface. It’s also good for fooling different applications that are expecting to have an ethernet connection available, even if you aren’t directly connected to a live ethernet network.

The type of loopback plug that you’ll use will depend on the type of interface that you’re connecting to. For example, you can have serial or RS-232 loopback plugs, some that are nine-pin and some that are 25-pin. There are separate loopback plugs that you would use for ethernet, T1, or even fiber connections. But the important thing to remember is that these are looping back traffic from one interface back into the same interface. These are not crossover cables, which allow us to connect different devices to each other.

In many environments there may be a wall of punch-down blocks. This is the intermediate section between a user’s workstation and the networking equipment that might be in a closet. We would take all of the cables from the users and punch them down into these punch-down blocks. But to be able to do that, we need the right punch-down tool. This might be punching down into a 66 block or a 110 block. And there are different connectors for the punch-down tool depending on the type of punch-down block that you’re using.

This can be a bit tedious, because we’re taking every single one of those connections, we’re splitting out those eight wires. We’re putting them into the eight different slots in that punch-down block. And then we’re using the punch-down tool to individually punch down those wires. It does help, though, that as you are pushing that wire into the punch-down block, the punch-down tool is also trimming the wire and making a neat connection in the block itself.

So you can see here, the punch-down tool has pushed all of these wires into the block. You can see the connectors inside of the block have pierced the plastic insulation on the outside, and making the copper connection, metal to metal, between the punch-down block and the wire itself. And you can see at the end of these that all of these ends have been nicely trimmed as it was punched down into the block.

If you’ve ever seen these large walls of punch-down blocks, you know that there is a lot to keep organized. And that’s why it’s important to always document exactly what wires are plugging into what connections. Your punch-down blocks may even have numbers associated with these. And you’re able to document exactly what wires are plugging into what connections.

Another important consideration is that you maintain the twists. The person that performed these punch-downs did a very good job of keeping the twists as close as possible to the punch-down block itself. You don’t want to have a large amount of wire that has been removed from the sheath and then spread out and then finally put into the punch-down block. Especially when you’re running higher speeds of ethernet, you want to make sure to maintain those twists as close as possible to the block.

With all of these connections, you’ll often find some documentation on paper that is written and posted right next to the punch-down blocks. Or sometimes there may be tags or information you can put on the wires themselves. Sometimes the wall itself will have writing from the person that performed the punch-down. So you may need to look closely behind the wires to see exactly what was written during the punch-down process.

We’ve talked a lot about copper tools that we need in our tool box. But we also need tools that allow us to see the wireless networks as well. A Wi-Fi analyzer is going to be able to see all of the different communication over your Wi-Fi network and give you feedback on signal strengths and exactly what frequencies may be in use on your network.

This might be a purpose-built appliance or device that you carry around with you that is specifically designed to provide Wi-Fi analysis. Or it may be additional software that you load on to an existing mobile device that gives you this capability. Either way, you’ll be able to see all of the frequencies that are in use in your area. You’ll see if there’s any errors or interference and be able to manage exactly how you can configure your wireless network to perform optimally.

****

Section 3: Hardware

****

3.1 – Cables and Adapters

Copper Network Cables (12:43)

Fiber Network Cables (3:29)

Video Cables (6:19)

Multipurpose Cables (6:58)

SATA Drive Cables (2:33)

PATA Drive Cables (3:50)

SCSI Drive Cables (6:31)

Adapters and Converters (2:54)

3.2 – Connectors

Connectors (8:41)

3.3 – Memory

~~~
Overview of Memory (7:51)
`````````````````````````

Memory Technologies (5:31)
``````````````````````````


3.4 - Storage
-------------
Storage Devices (9:22)
``````````````````````


RAID (7:20)
```````````


3.5 - Motherboards, CPUs, and Add-on Cards
------------------------------------------
Motherboard Form Factors (6:58)
```````````````````````````````


Motherboard Expansion Slots (11:46)
```````````````````````````````````


Motherboard Connectors (6:42)
`````````````````````````````


BIOS (5:26)
```````````


BIOS Options (7:32)
```````````````````


BIOS Security (4:13)
````````````````````


Installing BIOS Upgrades (5:12)
```````````````````````````````


CPU Features (10:03)
````````````````````


CPU Cooling (6:48)
``````````````````


Expansion Cards (4:55)
``````````````````````




3.6 - Peripherals
-----------------
Peripherals (12:35)
```````````````````



3.7 - Power
~~~

```
-----------
Computer Power (12:31)
``````````````````````

3.8 - Custom PCs

Custom Computer Systems (6:00)
~~~

3.9 - Common Devices

Common Devices (5:40)
`````````````````````

3.10 - SOHO Multifunction Devices

SOHO Multifunction Devices (10:31)
~~~

3.11 - Print Technologies

Laser Printers (10:06)
``````````````````````


Laser Printer Maintenance (4:38)
````````````````````````````````

Inkjet Printers (4:56)
``````````````````````


Inkjet Printer Maintenance (3:27)
`````````````````````````````````

Thermal Printers (2:49)
```````````````````````


Thermal Printer Maintenance (2:34)
``````````````````````````````````

Impact Printers (4:37)
``````````````````````


Impact Printer Maintenance (3:04)
`````````````````````````````````

Virtual and 3D Printers (5:17)
~~~

Section 4: Virtualization and Cloud Computing
===
```
~~~

## 4.1 - Cloud Computing

### Cloud Models (8:59)

### Cloud Services (6:12)

## 4.2 - Client-side Virtualization

### Client-side Virtualization (6:59)

# Section 5: Hardware and Network Troubleshooting

## 5.1 - Troubleshooting

### How to Troubleshoot (11:08)

## 5.2 - Troubleshooting Computer Hardware

### Troubleshooting Common Hardware Problems (18:18)

## 5.3 - Troubleshooting Storage

### Troubleshooting Hard Drives (6:44)

## 5.4 - Troubleshooting Displays

### Troubleshooting Video and Display Issues (7:12)

## 5.5 - Troubleshooting Mobile Devices

### Troubleshooting Laptops (7:28)

### Troubleshooting Mobile Devices (9:11)

### Device Disassembly Best Practices (4:00)

## 5.6 - Troubleshooting Printers

### Troubleshooting Printers (10:08)

~~~
5.7 - Troubleshooting Networks
------------------------------
Troubleshooting Networks (9:52)
```````````````````````````````


****
                  CompTIA 220-1002 A+ Training Videos
****

Section 1: Operating Systems
============================

1.1 - Operating Systems

Operating Systems Overview (14:16)
``````````````````````````````````


1.2 - Microsoft Windows
-----------------------
An Overview of Windows 7 (5:47)
```````````````````````````````


An Overview of Windows 8 and 8.1 (4:55)
```````````````````````````````````````


An Overview of Windows 10 (5:53)
````````````````````````````````

Windows in the Enterprise (4:23)
````````````````````````````````


1.3 - Installing Operating Systems
----------------------------------
Installing Operating Systems (19:07)
````````````````````````````````````


Installing and Upgrading Windows (9:51)
```````````````````````````````````````



1.4 - The Windows Command Line
------------------------------
Microsoft Command Line Tools (23:22)
````````````````````````````````````


Network Command Line Tools (22:06)
``````````````````````````````````



1.5 - Windows Features
----------------------
Windows Administrative Tools (18:10)
````````````````````````````````````


Windows Firewall with Advanced Security (5:26)
``````````````````````````````````````````````

~~~

~~~
System Configuration (4:05)
```````````````````````````


Task Manager (4:34)
```````````````````


Disk Management (9:03)
``````````````````````


System Utilities (16:51)
````````````````````````



1.6 - Windows Control Panel
---------------------------
The Windows Control Panel (13:42)
`````````````````````````````````



1.7 - Installation Concepts
---------------------------
Installing Applications (5:12)
``````````````````````````````



1.8 - Windows Networking
------------------------
HomeGroups, Workgroups, and Domains (5:58)
``````````````````````````````````````````


Windows Network Technologies (8:04)
```````````````````````````````````


Establishing Windows Network Connections (6:12)
```````````````````````````````````````````````


Configuring Windows Firewall (4:02)
```````````````````````````````````


Windows IP Address Configuration (5:28)
```````````````````````````````````````


Network Adapter Properties (5:55)
`````````````````````````````````


1.9 - macOS and Linux
---------------------
Best Practices for macOS (3:54)
```````````````````````````````

macOS Tools (4:42)
``````````````````


macOS Features (6:34)
`````````````````````
~~~

~~~

Best Practices for Linux (3:56)
```````````````````````````````


Linux Tools (3:19)
``````````````````


Basic Linux Commands (24:23)
````````````````````````````



Section 2: Security
===================
2.1 - Physical Security
-----------------------
Physical Security (8:36)
````````````````````````


2.2 - Logical Security
----------------------
Logical Security (25:23)
````````````````````````


2.3 - Wireless Security
-----------------------
Wireless Security (7:16)
````````````````````````


2.4 - Malware
-------------
Types of Malware (12:42)
````````````````````````


Anti-Malware Tools (6:15)
`````````````````````````



2.5 - Security Threats
----------------------
Social Engineering Attacks (9:59)
`````````````````````````````````


Denial of Service (4:02)
````````````````````````

Zero-day Attacks (3:39)
```````````````````````


Man-in-the-Middle (4:08)
````````````````````````


Brute Force Attacks (4:30)
``````````````````````````


Spoofing (3:12)
~~~

~~~~
```````````````


Non-compliant Systems (2:02)
````````````````````````````


2.6 - Windows Security

Windows Security Settings (9:03)
````````````````````````````````

2.7 - Workstation Security

Workstation Security Best Practices (10:45)
```````````````````````````````````````````


2.8 - Mobile Device Security
----------------------------
Securing Mobile Devices (8:39)
``````````````````````````````


2.9 - Data Destruction and Disposal
-----------------------------------
Data Destruction and Disposal (4:24)
````````````````````````````````````


2.10 - SOHO Network Security
----------------------------
Securing a SOHO Network (13:12)
```````````````````````````````



Section 3: Software Troubleshooting
===================================

3.1 - Troubleshooting Windows
-----------------------------
Troubleshooting Windows (15:26)
```````````````````````````````


Troubleshooting Solutions (18:17)
`````````````````````````````````



3.2 - Troubleshooting Security Issues
-------------------------------------
Troubleshooting Security Issues (8:24)
``````````````````````````````````````



3.3 - Malware Removal
---------------------
Removing Malware (8:28)
```````````````````````



3.4 - Troubleshooting Mobile Applications
~~~~

```
-----------------------------------------
Troubleshooting Mobile Apps (10:48)
```````````````````````````````````

3.5 – Troubleshooting Mobile Device Security
--------------------------------------------
Troubleshooting Mobile Device Security (6:12)
~~~

**************************************************************************
           Additional Study: Professor Messer’s A+ Study Groups
**************************************************************************

A+ Study Group Replays
2019 – 220-1001 A+ Study Group Sessions
February 2019
March 2019
April 2019
May 2019
June 2019

2019 – 220-1002 A+ Study Group Sessions
February 2019
March 2019
April 2019
May 2019
June 2019

========================================
Slots
-----
PCI

Hard Drives
-----------

Floppy Drives
-------------

USB Sticks??
------------

External Hard Drives
--------------------

CD and DVD
----------

Tapes
-----

Workstations
```
~~~

------------

Use

Thin Client
-----------
Use

Servers
-------
Use

Punch Down

https://www.google.com/search?q=punchdown+patch+panel&rlz=1C1CHBF_enUS783US783&source=lnms&tbm=isch&sa=X&ved=0ahUKEwigo-Tk34riAhXvRt8KHUj7ADoQ_AUIDygC&biw=1455&bih=717

HardwareInternshipClassNotes.pdf