



DSNE

Digital Signage Network Expert

Digital Signage Network Expert



1

Introduction

Digital Signage Network Expert

2

- The mandate of the DSNE program is to understand the fundamentals of how networks work and are constructed.
- By looking at the methodology behind network communication, and the hardware building blocks that make up any network, we can begin to address the vast array of different kinds of networks utilized in digital signage.
- In short, networks are the backbone of any digital signage system, and understanding how they work, and how we interact with them, will allow any system designer to successfully build or integrate into, any network.
- Our goal is to bring forth a group of digital signage network experts dedicated to creating quality and reliable networks to deliver the all-important digital signage content where and when it is needed.



 DSNE Digital Signage Network Expert

2

What is a Network?

Digital Signage Network Expert

- In the world of **IT (Information Technology)**, networking is the practice of linking two or more devices together for the purpose of sharing data and resources. Networks are built with a mix of hardware and software.
- Today, networks frequently incorporate many more components than just traditional computers. Smartphones, tablets, VOIP systems, videoconferencing, gaming, audiovisual equipment, and digital signage have all been connected to the network backbone as a valuable method of communication.



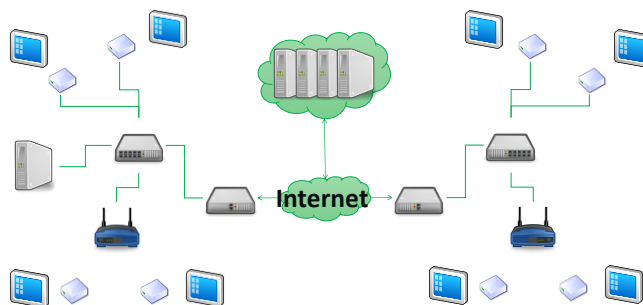
 **DSNE** Digital Signage Network Expert

3

The Network in Digital Signage

Digital Signage Network Expert

- **Every digital signage system is defined by its backbone, the network.**
- Connecting multiple sites together, or connecting multiple players within a single site, the network allows all the players to communicate with the central server, to receive content, schedules, and management.



 **DSNE** Digital Signage Network Expert

4

Network Architecture



5

Network Architecture Defined

Network Architecture

6

- **Network architecture** refers to the design of a network. It is a framework to understand the specification of the physical layout of the network, hardware components, functional organization, and operational principals.
- Network architecture will also define a physical medium of transmission of data, such as wired or wireless.
- Network architecture also helps define the geographic coverage of a network.
- To properly understand a network's architecture, we must examine the following concepts:
 - **LAN**
 - **WAN**
 - **Transmission Medium**
 - **Physical Topology**



 **DSNE** Digital Signage Network Expert

6

LAN – Local Area Network

Network Architecture

- **LAN**, or **Local Area Network**, is a very common term when discussing networks. It is often used interchangeably as a term to refer to the network itself.
- A LAN, as the name implies, covers a relatively limited area, typically within a single building or similar small geographic area.
- The most common transmission mediums for LANs are twisted pair cable (commonly known as Ethernet) or wireless radio broadcast (commonly known as Wi-Fi).
- A LAN is typically owned, used, and managed by a single organization.



 **DSNE** Digital Signage Network Expert

7

WAN – Wide Area Network

Network Architecture

- **WAN**, or **Wide Area Network**, is a less common term used to refer to a network spanning multiple sites or a large geographic area.
- A WAN is typically made up of a collection of LANs, dispersed among several buildings that may or may not be in geographic proximity to each other.
- Specialized hardware is used to connect the LANs together into a coherent single network inside the WAN.
- A WAN may be owned, used, and operated by a single organization, or can be shared under collective ownership.
- The Internet is the most well-known example of a WAN, and the largest and most used network in the world!
- **As of 2021, 4.93 BILLION people use the Internet each day!**



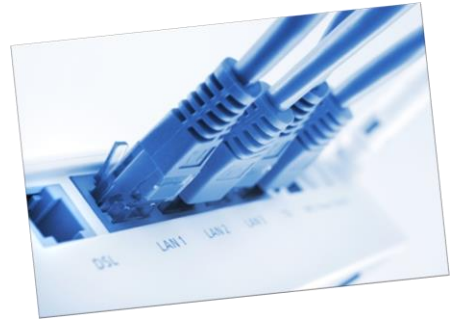
 **DSNE** Digital Signage Network Expert

8

Network Transmission Medium

Network Architecture

- The most common type of network today is based on **copper twisted pair cable**, also known as **category cable**.
- This uses a common protocol called **Ethernet** to manage transmission across the category cable, and to communicate with each device along the transmission path.
- Ethernet also defines a physical configuration for cable termination.
- Fiber optic cable may also be used for higher speed, larger bandwidth interconnects linking major parts of a network together.
- These cables provide the transmission medium for each device on a network to be interconnected and requires a physical link to the network itself.



 **DSNE** Digital Signage Network Expert

Network Transmission Medium

Network Architecture



- Modern networks also frequently incorporate wireless transmission of data, using radio frequency broadcasts.
- A **wireless local area network** or **WLAN**, is more commonly known by the name **Wi-Fi**.
- Wi-Fi spans several transmission standards that allow us to conduct the same kind of networking that happens over a wired Ethernet or fiber network over a wireless medium.
- Wi-Fi uses the exact same protocols as wired networking but uses a specific set of hardware to provide secure broadcast of information.

 **DSNE** Digital Signage Network Expert

Physical Topology

Network Architecture

- The networks **topology** represents its physical layout or structure from the point of view of data flow.
- This topology also helps define how each area and device will connect to the LAN or WAN, and how all distribution equipment such as switches, and routers will be laid out.
- Two common topologies are used today:
 - **Star topology**
 - **Tree topology**



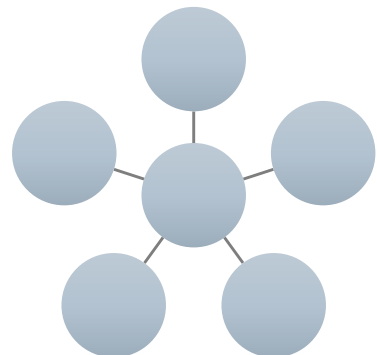
 **DSNE** Digital Signage Network Expert

11

Star Topology

Network Architecture

- A **star topology** is the most common type of network configuration.
- In a star network, each device is connected back to a central node with a point-to-point connection.
- The central node can be a hub, switch, or router, each with multiple ports to allow devices to connect.
- The central node acts a single point of distribution for data, and as a signal repeater.
- A star is the easiest type of network to implement, which is why it is most commonly found in homes and small offices.
- Multiple star networks can be combined by connecting the spoke of one star to the central hub of another star. This allows for simple expansions of a star network.



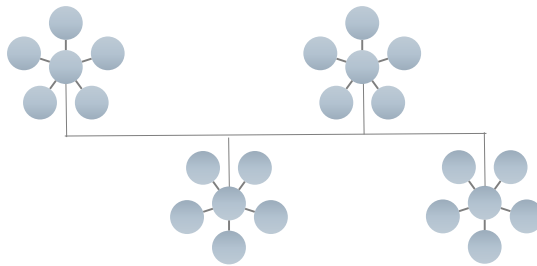
 **DSNE** Digital Signage Network Expert

12

Tree Topology

Network Architecture

- A **tree topology** is the common way a WAN like a large-scale corporate network or the Internet is constructed.
- A tree network is essentially a combination of multiple star networks connected to a common linear bus or backbone.
- This bus is often a specialized high speed or long-distance connection.



 **DSNE** Digital Signage Network Expert

13

Network Hardware

 **DSNE**
Digital Signage Network Expert

14

Networking Hardware Basics

Network Hardware

- To fully understand how a network is constructed, you must understand the basic hardware building blocks.
- All networks may contain these basic components in some combination:
 - Ethernet
 - Switch
 - Network Interface Card (NIC)
 - Power over Ethernet (PoE)
 - Router
 - Firewall



 **DSNE** Digital Signage Network Expert

15

Ethernet

Network Hardware

- **Ethernet** is the most popular physical layer LAN technology in use today.
- It defines the number of conductors that are required for a connection, termination of connectors, the performance thresholds that can be expected, and provides the framework for data transmission.
- Ethernet has evolved from the original **10 Mbps (10BASE-T)** standard into several forms, including **Fast Ethernet (100 Mbps, 100BASE-TX)** and **Gigabit Ethernet (1 Gbps, 1000BASE-T)**, and now **multi-Gigabit Ethernet (2.5, 5, 10, 25, and 40 Gbps - #BASE-T)**, and several fiber optic standards.
- Typically, higher speed implementations of Ethernet are backwards compatible with slower legacy standards and components, often specified as **10/100/1000**.
- Common Ethernet utilizes standard copper twisted pair category cables for connection.



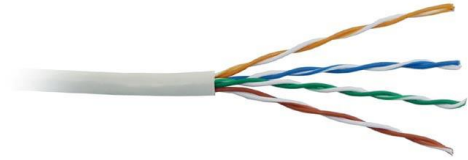
 **DSNE** Digital Signage Network Expert

16

Twisted Pair Cable

Network Hardware

- **Twisted pair cable** is a type of wiring in which two conductors of a single circuit are twisted together for the purposes of canceling out electromagnetic interference (EMI) from external sources; for instance, electromagnetic radiation and crosstalk between neighboring pairs.
- The two conductors carry equal and opposite signals, and the destination detects the difference between the two.
- Noise introduced into the conductors by electric or magnetic fields tend to affect both wires equally.
- The noise thus produces a common signal which can be canceled at the receiver.



 **DSNE** Digital Signage Network Expert

17

Categories of Cable

Network Hardware

- ANSI/EIA (American National Standards Institute/Electronic Industries Association) Standard 568 is the standard that specifies **categories** ("CAT" for short) of twisted pair cabling.
- The categories are defined in terms of the data rates they can sustain effectively, cable material, types of connectors, and junction blocks that need to be used with them.

Category	Frequency	Ethernet Supported	Connector	Distance
CAT 5	1-100MHz	10BASE-T, 10/100BASE-TX	8p8c, RJ45	100M
CAT 5E	1-100MHz	10/100/1000BASE-T	8p8c, RJ45	100M
CAT 6	1-250MHz	10/100/1000BASE-T	8p8c, RJ45	100M
CAT 6A	1-500MHz	10/100/1000BASE-T, 2.5/5/10GBASE T	8p8c, RJ45	100M
CAT 7	1-600MHz	10/100/1000BASE-T, 2.5/5/10GBASE T	GG45, TERA	100M
CAT 7A	1-1000MHz	10/100/1000BASE-T, 2.5/5/10GBASE T	GG45, TERA	100M
CAT 8	1-2000MHz	10/100/1000BASE-T, 2.5/5/10/20/40 GBASE T	GG45, TERA	30M

 **DSNE** Digital Signage Network Expert

18

Unshielded VS. Shielded Category Cable

Network Hardware

- Category cables also come in two types for each category, **unshielded twisted pair (UTP)** and **shielded twisted pair (STP)**. In both types of cable, the same type of twisted pair construction is used.
- Unshielded twisted pair is more common, it is lower cost, as no extra shielding is added to the cable.
- Shielded twisted pair contains an extra metallic shield, to help prevent interference. This shield can be foil or braid. The STP cable may also have extra foil shielding wrapped around individual pairs inside the cable.
- STP cable generally costs more but may be required for specific applications.



 **DSNE** Digital Signage Network Expert

19

Plenum VS. Non-Plenum Cable

Network Hardware

- From time to time, you may be asked to pull category cable through a wall, across a space above a ceiling, or below a floor. These are known as **plenum** spaces.
- Plenum spaces are typically those used for air return in HVAC systems, but in some jurisdictions, any cable not inside a conduit must comply.
- When doing so, it is important to use a properly rated cable, known as **plenum rated**, often labeled as **CMP**.
- According to **Article 800 of the National Electric Code (NEC)**, plenum cables must comply with specifications for flammability, smoke chemical content, and smoke density as set by **Underwriters Laboratories (UL)** and **National Fire Protection Association (NFPA)** testing methods.
- This means using special types of plastics for jackets and insulation, that are flame retardant, low smoke, and low toxicity.

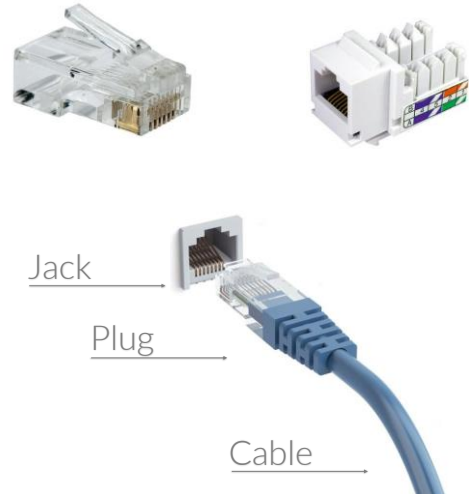
 **DSNE** Digital Signage Network Expert

20

Ethernet Termination

Network Hardware

- UTP or STP cables will commonly terminate into **RJ45 / 8P8C connectors**.
- **RJ45 connectors** (Registered Jack 45), also known as **8P8C connectors** (8 Position, 8 Contact), are used to create a modular connection system for UTP and STP cables up through CAT6A.
- RJ45 connectors come in a male **plug**, that may be crimped onto a category cable, and a female **jack** that typically terminates into a **punch down block**.
- A boot may be added to male plugs to help prevent the locking tab from snagging on anything, and to provide strain relief.
- RJ45 connectors also come in shielded varieties for extra interference protection.



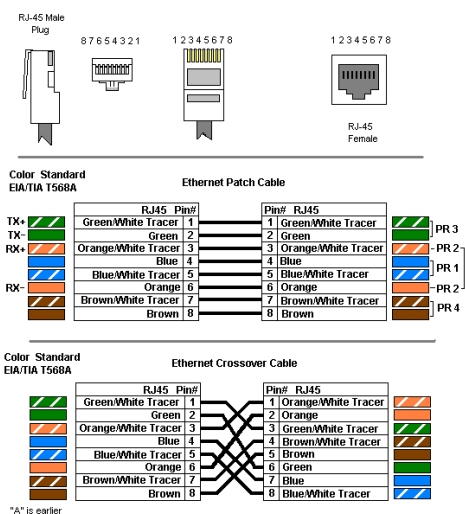
 **DSNE** Digital Signage Network Expert

21

Ethernet Termination

Network Hardware

1. Strip ½" of the category cable jacket
2. Separate the twisted wires
3. Arrange the separated pairs by color
4. Place the colored wires into the appropriate order as shown to the right
5. Insert into RJ45 plug as shown
6. Verify that no wire has shifted position inside the plug
7. Place into crimper and crimp connector onto wire
8. Test cable



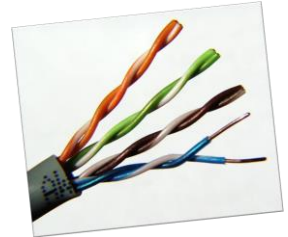
 **DSNE** Digital Signage Network Expert

22

Selecting Ethernet Cable

Network Hardware

- **When selecting a category cable, treat it no differently than you would selecting a cable for video.**
- Always select high quality cable, that is matched for your application.
- Category cable will come with jacket formulations, twist ratios, and configurations to tailor it to the application, such as direct burial, in wall or ceiling plenum, or shielded.
- High quality connectors with proper termination are another must. This affects overall network reliability and performance.
- Poorly terminated Ethernet cables can introduce crosstalk, or noise between lines, which slows the network speed.
- Do not untwist the cable more than absolutely necessary! The twists in the cable pairs are there to protect against interference and untwisting them can cause degraded performance.



 **DSNE** Digital Signage Network Expert

23

Ethernet Crossover Cables

Network Hardware

- **Crossover cables** are specific types of Ethernet cable, created with two sets of pins “flipped” compared to a standard Ethernet network cable.
- This was originally used to allow two devices to connect directly, without a switch.
- Most network devices today can automatically switch (usually called **autoswitching**) a port to replace this functionality.
- Some devices still use crossover cables for programming or terminal access, or to connect to another device.
- Check to see if any device you are using will require a crossover cable!



 **DSNE** Digital Signage Network Expert

24

Network Switches

Network Hardware

- A **network switch** (switch for short) is a hardware device with multiple Ethernet jacks, that joins multiple wired network devices together within one LAN.
- A switch has a limited amount of intelligence, to help it direct traffic from device to device. The switch will inspect data as it is received, determine the source and destination device, and forward it appropriately.
- Switches are typically classified by the speed they support, and the number of ports they have.
- Mainstream switches support either 10 Mbps, 100 Mbps, or Gigabit Ethernet standards. Increasingly, we are seeing multi-Gigabit capable switches, both for devices and for uplink.



 **DSNE** Digital Signage Network Expert

25

Network Switches

Network Hardware

- A **managed switch** is an advanced form of switch that has onboard processing not unlike a simple computer.
- This allows it to provide all the features of an unmanaged switch, and offer the ability to configure, manage, and monitor a LAN.
- This gives greater control over how data travels over the network, and who has access to it.



 **DSNE** Digital Signage Network Expert

26

Network Switches

Network Hardware

- **Some of the control options that a managed switch can provide:**
- Using **SNMP (Simple Network Management Protocol)** a managed switch can query and determine the health of the network or the status of a particular device. This data can be used to monitor the performance of the network and quickly detect and repair network problems.
- Using **QoS (Quality of Service)** a managed switch can prioritize network traffic by assigning critical traffic a higher priority. This ensures consistent network performance for delay-sensitive data like real-time voice or video communications.
- Managed switches can be used to create **virtual LANs (VLANs)** to isolate and restrict access to devices.
- Managed switches offer redundancy, using **STP (Spanning Tree Protocol)** to provide alternate paths between switches for network traffic.
- Managed switches may also offer **load balancing**, helping spread traffic so that no single switch will be overloaded.

 **DSNE** Digital Signage Network Expert

27

Network Switches

Network Hardware

- Switches, both managed and unmanaged, typically come in configurations up to 48 ports.
- This may appear to limit the number of available devices that can be connected; however, some switches have the ability to **stack**.
- Stacking means that the switch will be set up to operate with additional switches as a single unit.
- This is done via dedicated **uplink** ports, that may use interconnects like multi-gigabit Ethernet or fiber optics to provide for proper throughput (as if all ports are on a single switch).
- The interconnect between stacking switches will determine the bandwidth between each group of ports.
- For example, a switch with 24 Gigabit Ethernet ports, but only a 1Gbps interconnect for stacking, will severely limit the speed of the overall network, as having only 1Gbps for all devices on that switch to talk to devices on other switches in the stack reduces bandwidth.
- Always select switches with at least 10 gigabit interconnects, and above.

 **DSNE** Digital Signage Network Expert

28

Network Interface Cards

Network Hardware

- A **network interface card (NIC)**, or **network adapter** is the physical hardware inside a device that allows it to connect to the network.
- Often built into a computer, they may also be modular in the form of PCI/PCI Express cards that can be inserted as needed.
- A common way that NICs get added to devices today is via USB. Higher speed USB standards like USB 3.0 have provided a transport to connect the NIC without limiting its speed.
- NICs may be either wired Ethernet, or Wi-Fi.
- Some computers may have more than one NIC, to allow for connection to multiple networks, or to allow for both wired and wireless connections.



 **DSNE** Digital Signage Network Expert

29

Understanding Network Speeds

Network Hardware

- All LANs are rated for a specific speed, based on speed of the category of cable, and capacity of interconnecting hardware (such as switches) that are used.
- Network speeds are always rated in **bits per second**.
- This differs from how we measure the size of computer data files, in **bytes**.
- The difference may not appear significant but will impact understanding how long files will take to transfer.

Term	Unit	Description
Bit	b	Smallest unit in computing. Represents binary one or zero.
Byte	B	Represents a single character, comprised of 8 bits. (01000001 = A)
Kilobit	Kb	1000 (10^3) Bits.
Kilobyte	KB	1024 (2^{10}) Bytes
Megabit	Mb	1 000 000 (10^6) Bits
Megabyte	MB	1 048 576 (2^{20}) Bytes

- To convert from bits per second, to bytes per second, divide by 8. One byte is 8 bits.

 **DSNE** Digital Signage Network Expert

30

Understanding Network Speeds

Network Hardware

- **On average, LAN transfer rates are typically about 1/4th of the actual bandwidth.**
- LAN speeds can be influenced by the following factors:
 - Low quality LAN cable
 - Processing speed of switches and devices involved (typically older equipment has slower processing capabilities, which can drastically affect performance)
 - Storage speed - devices with slower hard drives will transfer content slower (because each packet of information must be written before it is considered to be transferred)

Theoretical Network Speed	1 Gb/sec (1000 Mb/sec)
Optimistic Transfer Rate	(1000 / 8) = 125 MB/sec
Likely Transfer Rates	~ 30 MB/sec

 **DSNE** Digital Signage Network Expert

31

Understanding Network Speeds

Network Hardware

- Ethernet commonly provides the following speeds:

Ethernet Standard	Max. Speed
10BASE T	10Mbps
10/100BASE TX	100Mbps
10/100/1000BASE T	1Gbps
10GBASE T	10Gbps

- When in a mixed device environment, with hardware components that support different speed standards, the network will limit its speed to accommodate the slowest device. This is known as **autonegotiation**.
- Autonegotiation also applies to setting duplex/simplex communications between devices.

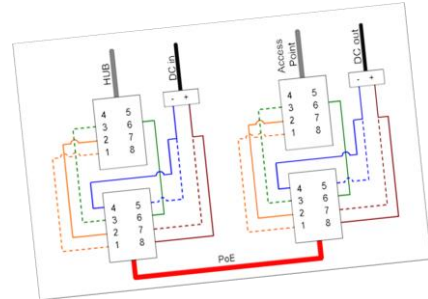
 **DSNE** Digital Signage Network Expert

32

Power over Ethernet (PoE)

Network Hardware

- **Power over Ethernet (PoE)** technology is a system to pass electrical power safely through Ethernet cabling without disrupting data traffic.
- Power is supplied into the Ethernet cable in common mode over two or more of the pairs of wires found in the cable.
- Power can come from the internal power supply within a PoE network device such as a switch or can be **injected** into a cable run by a special power supply device.
- **PoE requires the use of category 5 cable or higher.**



 **DSNE** Digital Signage Network Expert

33

Power over Ethernet (PoE)

Network Hardware

- The original **PoE 802.3af** standard allows for PoE to supply up to 15.4 watts of DC power (44V DC at 350 mA) to each device. Some power is lost in the cable, allowing for a guaranteed **12.95 watts** at the device.
- The **PoE+ 802.3at** standard, allows for up to **25.5 watts** of power.
- The latest **PoE++ 802.3bt** standard provides up to **71 watts** of power.
- This technology is especially useful for powering VOIP phones, wireless access points, IP cameras, remote Ethernet switches, embedded computers, thin clients, and even some smaller LCDs.

PoE vs PoE+ vs PoE++ Parameters				
	802.3af (802.3at Type 1) "PoE"	802.3at Type 2 "PoE+"	802.3bt Type 3 "PoE++"	802.3bt Type 4 "PoE++"
Power available	12.95 W	25.50 W	51 W	71 W
Maximum power	15.40 W	30.0 W	60 W	100 W
Voltage range	37.0–57.0 V	42.5–57.0 V	50.0–57.0 V	50.0–57.0 V
Maximum current	350 mA	600 mA	600 mA	960 mA
Power management	Three power class levels negotiated at initial connection	Four power class levels negotiated at initial connection, or 0.1 W steps negotiated continuously	Six power class levels negotiated at initial connection, or 0.1 W steps negotiated continuously	Eight power class levels negotiated at initial connection, or 0.1 W steps negotiated continuously

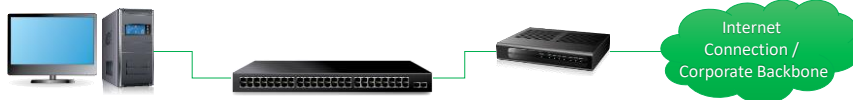
 **DSNE** Digital Signage Network Expert

34

Router

Network Hardware

- A **router** is a networking device that accepts traffic coming from one network and forwards it to a second network.
- A router is typically connected to two network connections (one for incoming and one for outgoing) spanning two separate networks, unlike a switch that will have many network connections connecting a single network.
- The most common use for a router is to connect a LAN to the Internet, translating traffic from a single publicly addressable IP address to the internal network.
- Routers may also be used to connect two completely separate LANs to each other, and route traffic between them.
- Routers may also be called a **gateway**, especially when it translates two different types of network together.



 **DSNE** Digital Signage Network Expert

35

Router

Network Hardware

- The most common types of router you will encounter are the **broadband router**, and the **wireless router**.
- These are single devices that contain several common components:
 - The **router** itself, with a **WAN port** for the internet connection
 - An integrated **4-5 port switch**, connected internally to the router
 - A **firewall** and **QoS** functions
 - A wireless router will also integrate a **wireless access point** for Wi-Fi functionality
 - Higher end or commercial oriented units may also allow for creation of **VPNs** and **VLANS**.
- These sorts of devices are mostly used for home networks, and small to medium business applications.
- Large scale networks will often separate out these functions into individual hardware components.



 **DSNE** Digital Signage Network Expert

36

Firewalls

Network Hardware

- A **firewall** is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.
- A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed to not be secure or trusted.
- Firewalls can be either dedicated hardware appliances, or a software application running on computer hardware.
- A firewall can apply to a whole network, or to an individual device.



 **DSNE** Digital Signage Network Expert

37

Wi-Fi

Wireless Networking

 **DSNE**
Digital Signage Network Expert

38

Wireless Networking

Wi-Fi

- **Wi-Fi**, or a **wireless local area network (WLAN)** is a methodology of utilizing two-way radio frequency communications to establish a network connection similar to a physical cable.
- Wi-Fi uses the same communications protocols as wired networking, so the only real difference is the transmission medium.
- A device's wireless adapter translates outgoing data into a radio signal and transmits it using an antenna.
- A wireless access point receives the signal and decodes it. The access point sends the data to the network using a physical, wired Ethernet connection.
- The process also works in reverse, with the access point receiving data from the network, translating it into a radio signal and sending it to the device's wireless adapter.



 **DSNE** Digital Signage Network Expert

39

Wi-Fi Standards

Wi-Fi

- There are a number of different Wi-Fi standards, based the **IEEE 802.11** standard.
- Each defines its own speed, geographic range, and frequency usage.
- The original standard was **802.11** providing 1 or 2 Mbps transmission in the 2.4 GHz band.
- From that, a number of enhanced standards were created, taking 802.11 and adding a letter to represent the standard, **A, B, G, N, AC**, and the new draft **AD**.
- The 5 and 5.8GHz bands were added on top of the 2.4GHz to improve performance. Additional bands are being tested for future 802.11 standards, such as AD in the 60 GHz range.
- Each new enhanced standard has added greater speed, range, and resistance to interference.



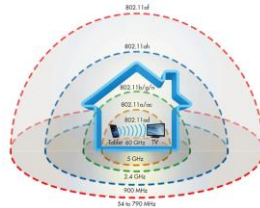
 **DSNE** Digital Signage Network Expert

40

Wi-Fi Standards

Wi-Fi

Standard	Speed (Mbps)	MIMO	Frequency	Range (Feet)
802.11A	54	No	5.8 GHz	60-100
802.11B	11	No	2.4 GHz	100-150
802.11G	54	No	2.4 GHz	150-250
802.11N	300	Up to 4	2.4 & 5 GHz	Up to 300
802.11AC	2600	Up to 8	2.4 & 5 GHz	Up to 300
802.11AD	4600	Up to 8	2.4, 5, 60 GHz	Up to 300 (2.5 /5 GHz), 15 (60 GHz)
802.11AX	9600	Up to 8	2.4, 5, 6 GHz	Up to 390



 **DSNE** Digital Signage Network Expert

41

Wi-Fi Standards – 2021 Update

Wi-Fi

- To simplify the Wi-Fi standards naming scheme, the Wi-Fi Alliance is instituting a new name system going forward, using simple numbers.
- 802.11n is now being called **Wi-Fi 4**
- 802.11ac is now being called **Wi-Fi 5**
- The new 802.11ax is being called **Wi-Fi 6 and 6E**
- The proposed **802.11ax (Wi-Fi 6 and 6E)** standard, also called High Efficiency WLAN, is intended to provide higher throughput (up to 4X that of Wi-Fi 5 / 802.11ac) in dense usage applications like hotels and stadiums.
- There are numerous new standards in planning beyond Wi-Fi 6, such as the draft **Wi-Fi 7 (802.11be)** promising up to 40Gbps speeds.



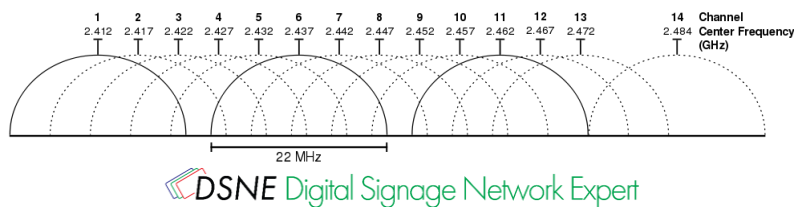
 **DSNE** Digital Signage Network Expert

42

Wireless Channels

Wi-Fi

- Within the 802.11 standards, each frequency range (2.4, 5, 5.8, 60 GHz, etc.) there are a set of specified **channels** at specific frequencies.
- Within the 2.4 GHz band, there are 14 channels of 20 MHz each, spaced 5 MHz apart.
- The 2.4 GHz channels mostly overlap each other, but 1, 6, and 11 are separated far enough apart to not overlap at all.
- Within the 5 GHz band, there is more free space, so there are 23 non overlapping 20 MHz channels.
- Selecting a non-overlapping channel, or a channel with lower traffic on it can improve your wireless throughput due to reduced interference.



DSNE Digital Signage Network Expert

43

Wireless Access Point

Wi-Fi

- A **wireless access point (WAP)**, also called a **hotspot**, is a device that acts as the physical bridge between wireless devices, and a wired network.
- The wireless access point broadcasts the 802.11 Wi-Fi network, and allows devices to connect to it, linking them to the network.
- Wireless access points may be built into home and small business routers or be stand alone devices.
- The wireless network that is created is identified by using an **SSID (Service Set Identifier)**, or a 32-character unique name that is both how a device can connect to the wireless network, and part of the protocol of communication for wireless devices.
- The SSID may be **broadcast** (visible to potential clients) or **hidden** (invisible to scans but allows connections if the SSID is known).



DSNE Digital Signage Network Expert

44

Antenna Technologies - MIMO

Wi-Fi

- **Multiple-Input Multiple-Output (MIMO)** technology is a wireless technology that uses multiple transmitters and receivers to transfer more data at the same time.
- MIMO technology takes advantage of a natural radio-wave phenomenon called multipath. With multipath, transmitted information bounces off walls, ceilings, and other objects, reaching the receiving antenna multiple times via different angles and at slightly different times.
- MIMO makes antennas work smarter by enabling them to combine data streams arriving from different paths and at different times to increase range and speed.
- More antennas usually equate to higher speeds. A wireless adapter with three antennas can have a speed of 600 mbps while an adapter with two antennas has a speed of 300 Mbps. The router also needs to have multiple antennas.
- New **multi-user MIMO (MU-MIMO)** increases this capacity by allowing multiple users access to multiple antennas. This is used in 802.11AD.



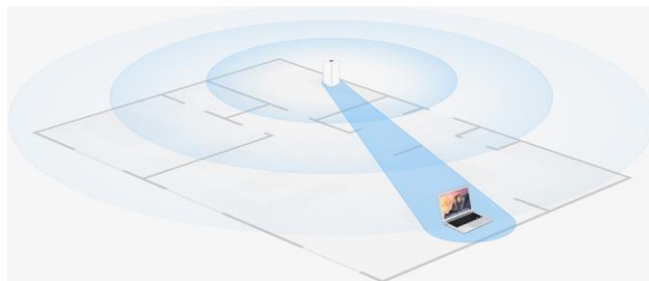
 **DSNE** Digital Signage Network Expert

45

Antenna Technologies - Beamforming

Wi-Fi

- Standard wireless systems broadcast their signal equally in all directions, regardless of where the receiver is located.
- **Beamforming** allows the wireless transmitter and receiver to communicate with each other to establish location relative to each other and determine the optimal signal path.
- The wireless transmission is then focused and targeted specifically to the receiver.



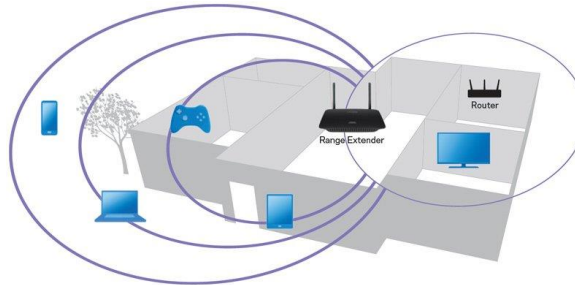
 **DSNE** Digital Signage Network Expert

46

Wireless Range Extender

Wi-Fi

- When a wireless access point does not provide enough range for a device to connect to it, a **wireless range extender** can be used to expand the reach of the network.
- A wireless range extender is basically a repeater, connecting to the original access point, and creating a new network with a new SSID.



 **DSNE** Digital Signage Network Expert

47

Wireless Mesh Networks

Wi-Fi

- A common practice, when a single wireless access point is not sufficient to cover an entire area (even with possible range extenders), is to use a **wireless mesh network**.
- A wireless mesh is essentially a network of routers without cabling in between nodes; mesh networks have a dedicated wireless communication channel (often called backhaul) that they use to communicate with each other.
- Devices will connect to a single wireless network but will be directed to whichever mesh node is the strongest signal for them. This allows for high coverage due to many nodes, but also higher speeds using shorter distances between nodes.



 **DSNE** Digital Signage Network Expert

48

Wireless Ethernet Bridge

Wi-Fi

- A **wireless Ethernet bridge** is a specialized network adapter, similar in design to a wireless access point, but intended to allow a device with no Wi-Fi capability to connect to a wireless network.
- The bridge will have one or more Ethernet ports, and will connect itself to the wireless network, providing the connection to wired only devices attached to it.
- Some access points can also be configured to be used as wireless Ethernet bridges.



 **DSNE** Digital Signage Network Expert

49

Wireless Reception

Wi-Fi

- Wireless reception on a W-Fi network is directly responsible for speed and reliability of the connection.
- A number of environmental factors can impact wireless reception:
 - A large number of other wireless networks
 - Other wireless equipment or electrical equipment producing interference
 - Physical obstructions such as walls or furniture (especially with a lot of metal)
- To get better reception, consider placing the wireless access point as high in the area as you can. Wireless signals travel better laterally, and down.
- Some wireless devices also offer replaceable antennas. 3rd party antennas can increase reception, shape signals, or allow relocating the antenna to avoid interference.



 **DSNE** Digital Signage Network Expert

50

Network Communications

How a Network Operates



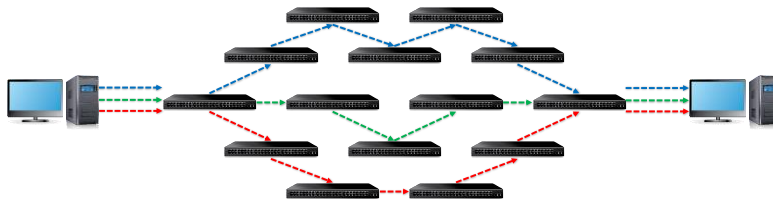
51

Packets: How Data is Transmitted

Network Communications

52

- A **packet** is a formatted unit of data carried by a network. All data is broken down into multiple packets before transmission.
- Packets may be routed across different parts of the network, allowing for non linear connections between endpoints, and the ability to route around a broken connection. This is known as **packet switching**.
- Packet switching allows the bitrate of the communication medium to be better shared among users.
- Packet format and size will be controlled by the protocol that the packet is intended to be used for.



DSNE Digital Signage Network Expert

52

Network Protocols: The Language of Networks

Network Communications

- In networking, the communication language used is called the **protocol**.
- A protocol defines a common set of rules and conventions for communication between network devices.
- A protocol includes formatting rules that specify how data is packaged.
- It also may include conventions like message acknowledgement or data compression.
- Networks offer multiple protocols to support specific applications.
- For example, **TCP/IP** is the most common protocol found on networks, and the protocol that drives the Internet.



 **DSNE** Digital Signage Network Expert

53

Network Protocols: The Language of Networks

Network Communications

- Protocols are layered on top of each other to create the final communication system:
 - **IP (Internet Protocol)** is the base packet protocol
 - **TCP (Transmission Control Protocol)** insures packet delivery through retransmission
 - **UDP (User Datagram Protocol)** sends messages with no guarantee of delivery
 - **HTTP (Hypertext Transfer Protocol)** delivers web content to the browser
 - **FTP (File Transfer Protocol)** allows for transfer of files
 - **RDP (Remote Desktop Protocol)** provides a remote-control system for Windows
 - **SIP (Session Initiation Protocol)** allows for video and audio-conferencing session startup



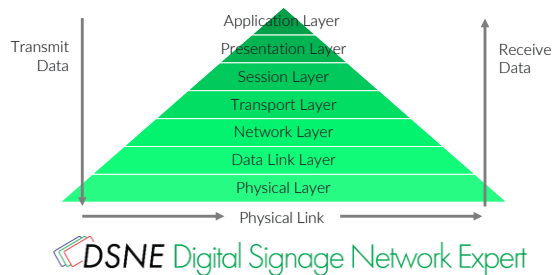
 **DSNE** Digital Signage Network Expert

54

OSI Model – Understanding Layers

Network Communications

- The **Open Systems Interconnection model (OSI Model)** is a conceptual model that characterizes and standardizes the communication functions of a network.
- Its goal is the interoperability of diverse networks with standard protocols.
- The model partitions a network into **7 layers**.
- A layer serves the layer above it and is served by the layer below it.
- For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that comprise the contents of that path.



55

OSI Model

Network Communications

Layer		Data unit	Function	Examples
Host layers	7. Application	Data	High-level APIs, including resource sharing, remote file access, directory services and virtual terminals	HTTP, FTP, SMTP, SSH, TELNET
	6. Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption	HTML, CSS, GIF
	5. Session		Managing communication sessions, i.e. continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes	RPC, PAP, SSL, SQL
	4. Transport	Segments	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing	TCP, UDP, NETBEUI
Media layers	3. Network	Packet/Datagram	Structuring and managing a multi-node network, including addressing, routing and traffic control	IPv4, IPv6, IPsec, AppleTalk, ICMP
	2. Data link	Bit/Frame	Reliable transmission of data frames between two nodes connected by a physical layer	PPP, IEEE 802.2, L2TP, MAC, DHCP, LLDP
	1. Physical	Bit	Transmission and reception of raw bit streams over a physical medium	Ethernet physical layer, DSL, USB, ISDN, DOCSIS

56

Identifying Devices: MAC Addresses

Network Communications

- In order to communicate properly with each device on a network, it must be identified and located.
- The **Media Access Control (MAC) address** is a unique identifying value associated with each device's network adapter.
- MAC addresses are also known as hardware addresses or physical addresses.
- MAC addresses are 12-digit hexadecimal numbers. MAC addresses are usually written as :
 - **MM:MM:MM:SS:SS:SS**
 - **MMMM-MMSS-SSSS**
- The first half of the MAC address contains the ID number of the adapter manufacturer. These IDs are regulated by an Internet standards body.
- The second half of the MAC address represents the serial number assigned to the adapter. For example:
 - **00:A0:C9:14:C8:29**
 - **The prefix 00A0C9 indicates the manufacturer is Intel Corporation.**
- IP networks maintain a map of IP addresses of a device, and its MAC address.

 **DSNE** Digital Signage Network Expert

57

IP Address Basics

Network Communications

- **On a network, every piece of equipment needs to have an address to allow other pieces of equipment to find and communicate with it.**
- This address is known as an **IP address**.
- IP addresses take the form of 4 groups of 3 numbers, such as "192.168.1.1"
- Each group of numbers makes up 8 bits of information, so it is known as an **octet**.
- Each octet value can range from 0-255.
- An IP address is used to communicate between devices much like how the mail works.

 **DSNE** Digital Signage Network Expert

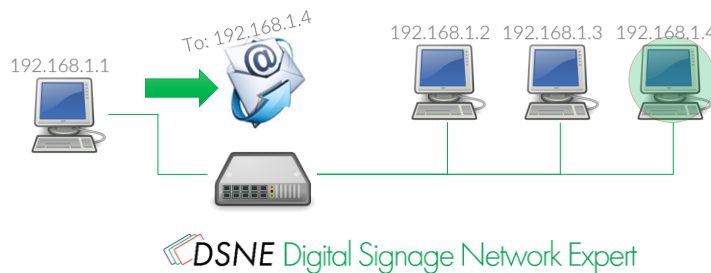


58

IP Address Basics

Network Communications

- To send a letter to someone (a packet of data), you must know the recipients address (IP address).
- Then you can write the address on the envelope (packet of data) and put it in the mail (send it over the network).
- The post office (router) uses that address (IP address) to determine where to send your letter (packet of data), and who to deliver it to.
- All information sent inside a network is broken into packets that are configured and sent in this manner.



59

IP Address Assignment

Network Communications

- **There are two types of IP address assignment in a network:**
- **Static**
 - This means that the device has a user specified IP address, that will never change unless done so by the user.
- **DHCP (Dynamic Host Control Protocol)**
 - This type of IP address will be assigned automatically by the network, from a designated pool of addresses.



DSNE Digital Signage Network Expert

60

DHCP IP Address Assignment

Network Communications

- **Dynamic Host Configuration Protocol (DHCP)** automates network-parameter assignment to network devices from one or more DHCP servers. Even in small networks, DHCP is useful because it can make it easy to add new machines to the network.
- When a DHCP-configured client connects to a network, the DHCP client sends a broadcast query requesting necessary information from a DHCP server.
- The DHCP server manages a pool of IP addresses and information about client configuration parameters such as default gateway, the DNS servers, and so forth.
- On receiving a valid request, the server assigns the computer an IP address, a lease (length of time the allocation is valid), and other IP configuration parameters, such as the subnet mask and the default gateway. The query is typically initiated immediately after booting and must complete before the client can initiate IP-based communication with other hosts.



 **DSNE** Digital Signage Network Expert

61

DHCP IP Address Assignment

Network Communications

- **Depending on implementation, the DHCP server may have three methods of allocating IP-addresses:**
- **Dynamic allocation:** A network administrator assigns a range of IP addresses to DHCP, and each client computer on the LAN has its IP software configured to request an IP address from the DHCP server during network initialization.
- The request-and-grant process uses a lease concept with a controllable time period, allowing the DHCP server to reclaim (and then reallocate) IP addresses that are not renewed (dynamic re-use of IP addresses).
- **Automatic allocation:** The DHCP server permanently assigns a free IP address to a requesting client from the range defined by the administrator.
- This is like dynamic allocation, but the DHCP server keeps a table of past IP address assignments, based on MAC address, so that it can preferentially assign to a client the same IP address that the client previously had.
- **Static allocation:** The DHCP server allocates an IP address based on a table with MAC address/IP address pairs, which are manually filled in (perhaps by a network administrator).
- Only requesting clients with a MAC address listed in this table will be allocated an IP address. This is commonly called IP address reservation in most network software and hardware.

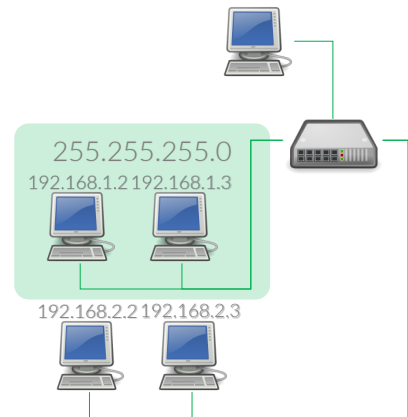
 **DSNE** Digital Signage Network Expert

62

Subnet / Subnet Mask

Network Communications

- Users can divide a physical network into multiple logical segments known as subnetworks or **subnets**.
- A number like an IP address known as a **subnet mask** is used to identify which subnet a device is on and help route traffic to it.
- Network devices use the IP address targets and defined subnet mask to determine if the network the host is on is a local subnet, or a remote network.
- This is important because devices act differently depending on the result.
- If the subnet is local, the device will send a request to retrieve the hardware address of the system.
- If the address is found to be on a remote network, then the network device routes packets to the gateway in it's routing table that is set to handle that network.
- If no routing table entry is found matching that network, the packets are routed to the default route.



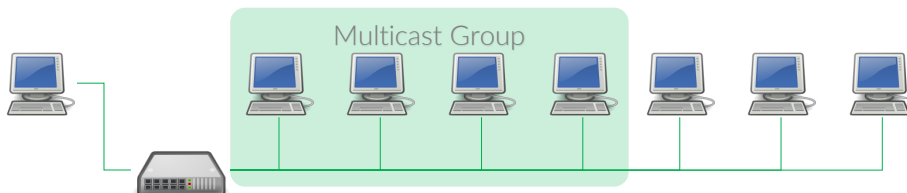
 **DSNE** Digital Signage Network Expert

63

IP Multicast

Network Communications

- **IP multicast** is a technique for **one-to-many** and **many-to-many** real-time communication over an IP infrastructure in a network.
- Multicast uses network infrastructure efficiently by requiring the **source device** to send a packet only once, even if it needs to be delivered to a large number of **receiver devices**.
- Compatible multicast network switches and routers replicate data packets and send them to multiple receivers so that data is sent over each link of the network only once.
- IP multicast requires neither prior knowledge of a receiver's identity nor prior knowledge of the number of receivers.



 **DSNE** Digital Signage Network Expert

64

IP Multicast

Network Communications

- An **IP multicast group address** is used by sources and the receivers to send and receive multicast messages.
- Sources use the group address as the IP destination address in their data packets.
- Receivers use this group address to inform the network that they are interested in receiving packets sent to that group.
- For example, if content is associated with group 239.1.1.1, the source will send data packets destined to 239.1.1.1. Receivers for that content will inform the network that they are interested in receiving data packets sent to the group 239.1.1.1. The receiver joins 239.1.1.1.
- The protocol typically used by receivers to join a group is called the **Internet Group Management Protocol (IGMP)**.

 **DSNE** Digital Signage Network Expert

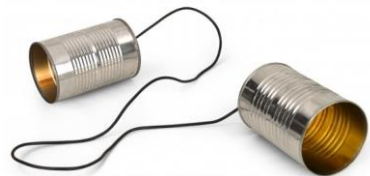
65

TCP – Transmission Control Protocol

Network Communications

- **TCP (Transmission Control Protocol)** is the most common method in which devices communicate over IP. Paired together, they are often referred to as **TCP/IP**.
- TCP is best described as a conversation between two devices. A computer viewing a web page is one of the best examples of TCP communication:

- **Client Computer:** I'd like to see your web page.
- **Web Server:** Sure, I'll start sending it to you.
- **Client Computer:** Thanks.
- **Web Server:** Here's a graphic. Did you receive it?
- **Client Computer:** I sure did. What's next?
- **Web Server:** Here's some text. Did you receive it?
- **Client Computer:** I sure did. What's next?
- **Web Server:** There's nothing else to send you.
- **Client Computer:** Thanks!



- Typically, TCP communication begins with a client requesting the resources of a server. The server replies, and the client computer acknowledges the reply. Each time the server sends information, the client computer acknowledges that the information was received, and more importantly, received correctly.

 **DSNE** Digital Signage Network Expert

66

TCP – Transmission Control Protocol

Network Communications

- TCP is the dominant communication protocol, because it is a reliable protocol. If a client computer does not get a transmission in time, or a server does not receive an acknowledgement, then it will try again. Consider our previous example:
 - **Web Server:** Here's a graphic. Did you receive it?
 - **Client Computer:**
 - **Web Server:** Here's a graphic. Did you receive it?
 - **Client Computer:** I sure did. What's next?
- This is why sometimes you will see a web page try to load, but eventually give up with an error.
- Typically, disruptions in TCP/IP networks are caused by too many requests to a given server, or a disruption in the route used to transmit information back and forth.
- While TCP is the most common form of transmission over an IP network, there are other protocols, each with their own advantages and disadvantages.



67

HTTP – Hypertext Transfer Protocol

Network Communications

- **HTTP (Hypertext Transfer Protocol)** is the underlying protocol used by the World Wide Web.
- HTTP defines how messages are formatted and transmitted, and what actions Web **servers** and **browsers** should take in response to various commands.
- For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page.
- The other main standard that controls how the World Wide Web works is **HTML (Hypertext Markup Language)**, which covers how Web pages are formatted and displayed.



68

FTP – File Transfer Protocol

Network Communications

- **File Transfer Protocol (FTP)** is the commonly used protocol for exchanging files over the Internet.
- FTP uses the Internet's TCP/IP protocols to enable reliable and efficient data transfer.
- FTP uses a client-server architecture to transfer files to a user's computer.
- The user's computer is called the **local host** and is connected to the Internet, running a **FTP client**. The second machine, called the **remote host**, is running an **FTP server** also connected to the Internet.
- The local host machine connects to the remote host's IP address.
- The user would enter a username/password (or use anonymous).
- FTP software may have a GUI, allowing users to drag and drop files between the remote and local host. If not, a series of FTP commands are used to log in to the remote host and transfer files between the machines.



 **DSNE** Digital Signage Network Expert

69

Understanding Ports

Network Communications

- As we've seen, devices on a network use protocols to talk to one another.
- But there's a lot of devices talking to each other at the same time, using a lot of different protocols!
- To keep things organized and separate, **ports** are necessary.



 **DSNE** Digital Signage Network Expert

70

Understanding Ports

Network Communications

- A good way to think about ports, is that each network connection is a honeycomb.
- A honeycomb is made up of many different cells. Each cell represents an individual port.
- Specific applications under specific protocols are assigned to use certain ports, to help organize all of the traffic passing through a network.
- Not all ports may be in use at the same time. Many applications send traffic over a few specific ports.
- **Each port will be assigned a unique number, from 1-65535.**



 **DSNE** Digital Signage Network Expert

71

Understanding Ports

Network Communications

- On any given device, the ports will be either **open** or **closed**, based on security policies, and software settings.
- When a device is waiting for an incoming request to be received over a certain port, it is said to be **listening** on that port.
- Ports may also be closed, or traffic regulated and limited as it passes through them.
- Imagine if all 65,535 ports were open! The device would be at risk from intrusion because nothing would stop traffic from coming in through an open port.
- Open ports are considered a security risk, because it is impossible to determine if the incoming traffic is dangerous, or not.
- This is why system administrators frequently close unused or unneeded ports.



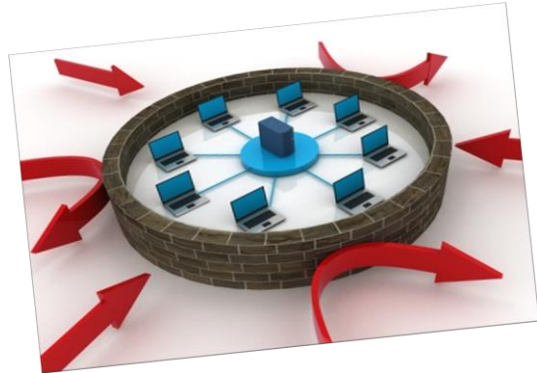
 **DSNE** Digital Signage Network Expert

72

Common Ports and Their Uses

Network Communications

- Port 80 – HTTP
- Port 443 – SSL/HTTPS
- Port 21 – FTP
- Port 22 – SSH/SFTP
- Port 25 – SMTP
- Port 110 – POP3
- Port 143 – IMAP
- Port 3389 – RDP
- Port 5900 – VNC



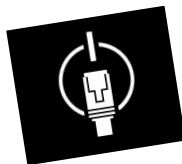
 **DSNE** Digital Signage Network Expert

73

Wake on LAN (WoL)

Network Communications

- **Wake-on-LAN (WoL)** is an industry standard protocol for waking computers up from a very low power mode remotely. The definition of “low power mode” has changed a bit over time, but we can take it to mean while the computer is “off” and has access to a power source. The protocol also allows for a supplementary Wake-on-Wireless-LAN ability as well.
- WoL-enabled devices essentially wait for a “**magic packet**” to arrive that includes the devices’ MAC address.
- These magic packets are sent over the network by software, a router, or even a website.
- The typical ports used for WoL magic packets are UDP 7 and 9.
- Because your device is actively listening for a packet, its network interface must remain active, so power consumption may be higher than if it is truly “off”.



 **DSNE** Digital Signage Network Expert

74

SNMP: Remote Monitoring

Network Communications

- **Simple Network Management Protocol (SNMP)** is a standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.
- Devices that typically support SNMP include routers, switches, computers, printers, and many other devices.
- SNMP is widely used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.
- SNMP allows for status and health data to be provided to management systems, and allow them to change different configurations and settings, and perform tasks like rebooting.



 **DSNE** Digital Signage Network Expert

75

Virtual Network Computing (VNC)

Network Communications

- In dealing with computers, **Virtual Network Computing (VNC)** is a graphical desktop sharing system that allows a user to remotely control another computer.
- It transmits the keyboard and mouse events from one computer to another, relaying the graphical screen updates back in the other direction, over a network.
- VNC is platform-independent – there are clients and servers for many GUI-based operating systems and for Java.
- Popular uses for this technology include remote technical support and accessing files on one's work computer from one's home computer, or vice versa.
- VNC consists of two components:
 - **VNC Server:** the software program that listens for incoming connections and provides control of the computer it is installed on.
 - **VNC Client:** the software program that connects to a VNC Server, and relays keyboard and mouse data from the computer it is installed on, while displaying video from the VNC Server.



 **DSNE** Digital Signage Network Expert

76

Internet Communications

World Wide Networking



77

Internet IP Addresses

Internet Communications

78

- The fundamentals of IP addresses that have been already discussed cover communication inside a network, but what about when we have to send information from one network to another over the Internet?
- Each Internet connection has its own IP address, called a **public IP address**, because it is visible to the Internet as a whole.
- This public IP address can be used to send information to a specific network out on the Internet, not unlike making a phone call.
- This will allow us to connect a public IP address to a **private IP address**.



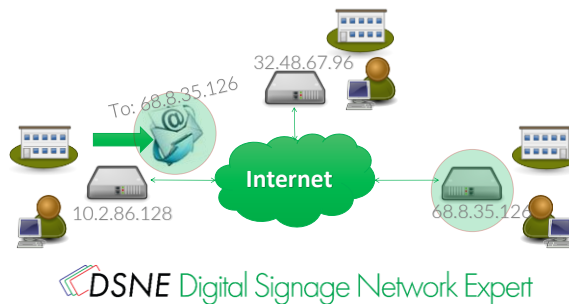
 DSNE Digital Signage Network Expert

78

Internet IP Addresses

Internet Communications

- If you want to make a call (send data packets) to someone else, you use their phone number to call them (connect to their public IP address). Then you can carry on a conversation (transmit data across the Internet).
- Networks will use this public IP address like a phone number, allowing you to “call” a specific recipient.
- The router is the device on a network that translates information from outside sources (the public IP address) to internal receivers (private IP addresses) and vice versa.

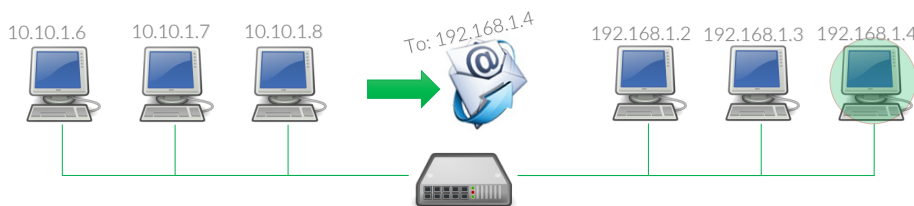


79

Internet IP Addresses

Internet Communications

- You may also encounter a system that has multiple private networks internal to an organization, joined together by **gateways**.
- The gateway acts like a router, analyzing the address information on the IP packets, and directing them to the appropriate network.



80

DNS

Internet Communications

- The **Domain Name System (DNS)** is a hierarchical naming system for computers, services, or any resource connected to the Internet or a private network.
- It associates various information with **domain names** assigned to each of the participants.
- Most importantly, it translates domain names meaningful to users into the IP addresses associated with networking equipment.
- An often-used analogy to explain the Domain Name System is that it serves as the "phone book" for the Internet.
- For example, **www.example.com translates to 192.0.32.10.**



 **DSNE** Digital Signage Network Expert

81

Firewall – Filtering Incoming Traffic

Internet Communications

- A **firewall** is a dedicated hardware appliance, or software running on a computer (or a combination of both) which inspects network traffic passing through it and denies or permits passage based on a set of rules.
- It is normally placed between a protected network and an unprotected network and acts like a gate to protect assets to ensure that nothing private goes out and nothing malicious comes in.
- A firewall's basic task is to regulate some of the flow of traffic between computer networks of different trust levels.
- Typical examples are the Internet which is a zone with no trust and an internal network which is a zone of higher trust. A zone with an intermediate trust level, situated between the Internet and a trusted internal network, is often referred to as a "perimeter network" or **demilitarized zone (DMZ)**.



 **DSNE** Digital Signage Network Expert

82

Types of Firewall

Internet Communications

- There are several types of firewall techniques that will prevent potentially harmful information from getting through:
- **Packet Filter**
 - Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure.
- **Application Gateway**
 - Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective but can impose a performance degradation.
- **Circuit-level Gateway**
 - Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
- In practice, many firewalls use two or more of these techniques in concert.
- A firewall is considered a first line of defense in protecting private information.

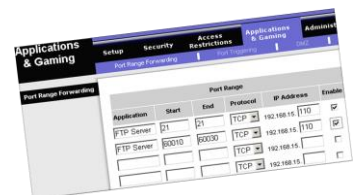
 **DSNE** Digital Signage Network Expert

83

Port Forwarding

Internet Communications

- **Port forwarding** refers to the ability of a router or gateway to accept incoming traffic to it's external IP address and a specific port, and relay that traffic to a specific internal IP address and port controlled by rules configured by the administrator.
- The technique is used to permit communications by external devices with specific devices within a private LAN.
- For example:
 - Running a public HTTP server within a LAN (port 80)
 - Permitting SSH access on the LAN from the Internet (port 22)
 - Permitting FTP access to hosts on a LAN from the Internet (port 21)
- Some common caveats with port forwarding include:
 - Only one networked device can use a specific forwarded port at one time.
 - Traditional port forwarding allows the entire world access to the forwarded port, slightly reducing network security.



Application	Start	End	Protocol	IP Address	Enable
FTP Server	21	21	TCP	192.168.15.110	<input checked="" type="checkbox"/>
FTP Server	80010	80030	TCP	192.168.15.110	<input checked="" type="checkbox"/>
			TCP	192.168.15.110	<input type="checkbox"/>

 **DSNE** Digital Signage Network Expert

84

Proxies

Internet Communications

- In computer networks, a **proxy server** or **proxy** is a server (a computer or an application) that acts as an intermediary for requests from devices seeking resources from other servers.
- A device connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity.
- A proxy server may reside at various points between the user's device and destination servers or the Internet.
 - A proxy server that passes requests and responses unmodified is usually called a **gateway** or sometimes a **tunneling proxy**.
 - A **forward proxy** is an Internet-facing proxy used to retrieve from a wide range of sources (in most cases anywhere on the Internet).
 - A **reverse proxy** is usually an Internet-facing proxy used as a front-end to control and protect access to a server on a private network. A reverse proxy commonly also performs tasks such as load-balancing, authentication, decryption or caching.

 **DSNE** Digital Signage Network Expert

85

Uses for Proxies

Internet Communications

- **Content-control software**
 - A content-filtering web proxy server provides administrative control over the content that may be relayed in one or both directions through the proxy. It is commonly used in both commercial and non-commercial organizations (especially schools) to ensure that Internet usage conforms to acceptable use policy.
- **Filtering of encrypted data**
 - Web filtering proxies are not able to peer inside secure sockets HTTP transactions, assuming the chain-of-trust of SSL/TLS has not been tampered with.
- **Logging and eavesdropping**
 - Proxies can be installed in order to eavesdrop upon the data-flow between client machines and the web. All content sent or accessed – including passwords submitted and cookies used – can be captured and analyzed by the proxy operator.

 **DSNE** Digital Signage Network Expert

86

Uses for Proxies

Internet Communications

- **Improving performance**

- A caching proxy server accelerates service requests by retrieving content saved from a previous request made by the same client or even other clients. Caching proxies keep local copies of frequently requested resources, allowing large organizations to significantly reduce their upstream bandwidth usage and costs, while significantly increasing performance.

- **Security**

- A proxy can keep the internal network structure of a company secret by using network address translation, which can help the security of the internal network.

- **Cross-domain resources**

- Proxies allow web sites to make web requests to externally hosted resources (e.g. images, music files, etc.) when cross-domain restrictions prohibit the web site from linking directly to the outside domains.

 **DSNE** Digital Signage Network Expert

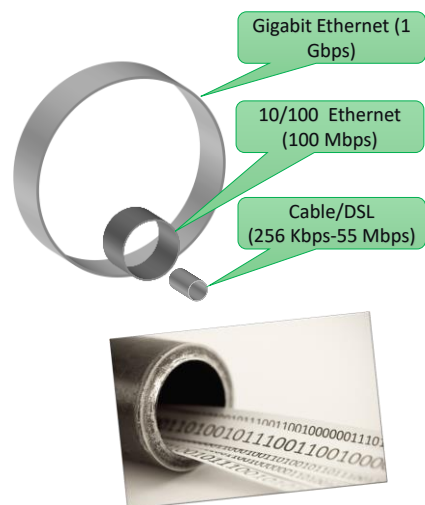
87

The Mystery of Bandwidth

Internet Communications

- **Bandwidth is the measure of both speed and capacity within a given network connection.**

- Bandwidth is expressed in terms of an amount of data that can be transmitted across a network in a given time period, usually as **megabits (Mbps)** or **kilobits (Kbps)** per second.
- The more bandwidth available, the higher amount of data can be transmitted per second, the faster the connection appears to operate.
- Thus the more bandwidth a network has, the more data that can be transmitted.



 **DSNE** Digital Signage Network Expert

88

The Mystery of Bandwidth

Internet Communications

- Bandwidth is always broken down into two measurements:
 - **Upstream bandwidth**
 - **Downstream bandwidth**
- Upstream bandwidth is the ability of a given network connection to transmit data out to the network.
- Downstream bandwidth is the capacity of a given network to receive data.



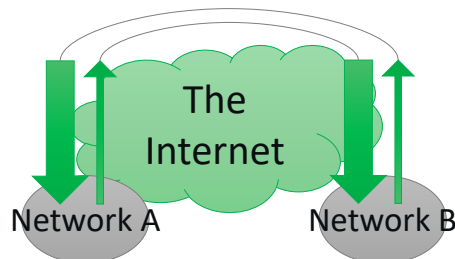
 **DSNE** Digital Signage Network Expert

89

The Mystery of Bandwidth

Internet Communications

- Inside a network, the bandwidth is usually **symmetrical**, meaning upstream and downstream are identical in speed.
- When looking at an internet connection, the upstream and downstream are **asymmetrical**, meaning one is larger than the other.
- Downstream speed is usually higher than upstream speed, and getting higher upstream speeds is typically expensive.



 **DSNE** Digital Signage Network Expert

90

The Mystery of Bandwidth

Internet Communications

- **The most important thing regarding upstream and downstream: Any given operation is only going to be as fast as upstream of a given connection allows.**
- Example: If you're downloading a file via your 512 Kbps connection from a server that has a 10000 Kbps upstream (10 Mbit) you're going to cap your speed at about 50 Kilobytes/sec. However, if that sever only has 100 Kbps upstream, your speed will cap out at roughly 10-12 Kilobytes/sec.
- Upstream is the deciding factor when discussing file transfer rates.



 **DSNE** Digital Signage Network Expert

91

Transfer Rates – Calculating Speed

Internet Communications

- The difference between bits and bytes is subtle and can be quite confusing.
- To convert bits to bytes, simply divide by 8. (512Kb / 8 = 64KB)
- Typically, bits are used when ISP's describe the speed of their internet connections to make them sound more appealing. Consumers will typically compare numbers and choose the largest number their budget permits.
- A 512Kb/sec connection is the same speed as a 64KB/sec connection. Assuming both plans are the same price, a user would probably pick the 512Kb/sec connection.

Term	Unit	Description
Bit	b	Smallest unit in computing. Represents binary one or zero.
Byte	B	Represents a single character, comprised of 8 bits. (01000001 = A)
Kilobit	Kb	1000 (10 ³) Bits.
Kilobyte	KB	1024 (2 ¹⁰) Bytes
Megabit	Mb	1 000 000 (10 ⁶) Bits
Megabyte	MB	1 048 576 (2 ²⁰) Bytes

 **DSNE** Digital Signage Network Expert

92

Transfer Rates – Line Factors

Internet Communications

- **Bandwidth is limited by the type of connection, and the hardware involved in sending it.**
- **Limiting factors include:**
 - Line noise can reduce the effectiveness of a high-speed bandwidth. Typically, noise is introduced by too many splitters before the connection leaving the building, or a poor-quality cable being installed by the provider.
 - Older hardware in particular does not necessarily have the ability to keep up with faster connections. This is typically more common in consumer hardware than commercial grade.
 - The type of traffic being sent / received - some ISP's will throttle traffic if it is not deemed to be 'acceptable' or 'regular' traffic.
 - Internet traffic in general. Large events can cause a lot of traffic, which increases the response time of any traffic using major routes.

 **DSNE** Digital Signage Network Expert

93

Bandwidth in the Real World

Internet Communications

- The best way to consider bandwidth is to think of the Internet connection as a door, and data as the people passing through it.
- Ordinarily, people flow through a door one at a time.
- However, if people are impatient, people can try and squeeze through the door simultaneously. This doesn't work too well.
- Now add that you've got people going in and out of the door at the same time – this is how bandwidth works.
- The first solution is often the most effective. Get a bigger door - more bandwidth!
- That may not be enough, as people have to pass through several doors to get to their destination.
- If a door has too many people trying to get through, it will become congested – and slowing traffic through that door, regardless of the eventual destination.

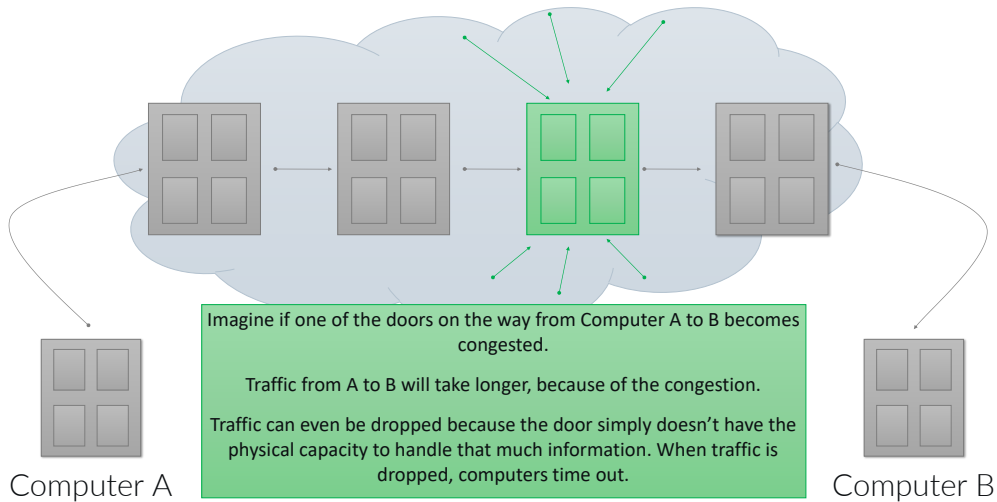


 **DSNE** Digital Signage Network Expert

94

Bandwidth in the Real World

Internet Communications



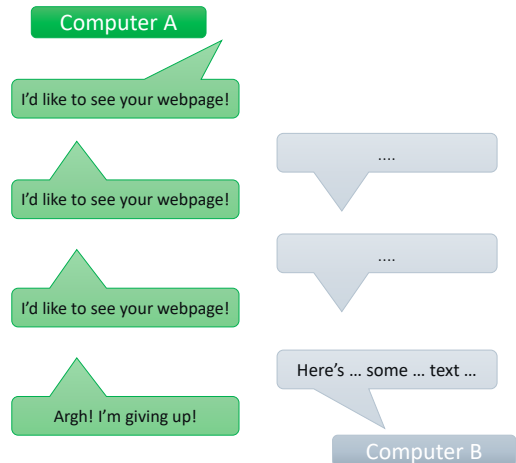
 **DSNE** Digital Signage Network Expert

95

Bandwidth in the Real World

Internet Communications

- Consider the conversation we used as an example for TCP, if part of the traffic times out:
- It's entirely possible that computer B is receiving A's requests to see the page – however, since one of the 'doors' is congested, A may not see B's response at all.
- Computer A will try a few times to establish a conversation with B, but will eventually give up if it doesn't receive a full statement from B.
- Congestion increases response time. Congestion is a natural part of the Internet and cannot be completely avoided.
- Things that can avoid congestion:
 - Laying private fiber between locations
 - Using high bandwidth connections with Quality of Service guarantees
 - Using packet shaping devices that reduce the overall packet size before transmission, and then reconstruct the packet before presentation



 **DSNE** Digital Signage Network Expert

96

Quality of Service Standards

Internet Communications

- In the field of networking, the traffic engineering term **quality of service (QoS)** is the ability within a network to provide different priority to different applications, users, or data flows.
- It may also be used as a contractual term for a service provider to guarantee a certain level of performance as part of an **SLA (Service Level Agreement)**.
- For example, a required bit rate, delay, jitter, packet dropping probability and/or bit error rate may be guaranteed.
- Quality of service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as VOIP and IPTV, since these often require fixed bit rate and are delay sensitive, and in networks where the capacity is a limited resource.



 **DSNE** Digital Signage Network Expert

97

Quality of Service Standards

Internet Communications

- When looking at packet-switched networks, Quality of Service is affected by various factors, which can be divided into "human" and "technical" factors.
- Human factors include: stability of service, availability of service, delays, user information.
- Technical factors include: reliability, scalability, effectiveness, maintainability, Grade of Service, etc.
- Many things can happen to packets as they travel from origin to destination, resulting in the following problems as seen from the point of view of the sender and receiver:
- **Throughput**
 - Due to varying load from other users sharing the same network resources, the bit-rate (the maximum throughput) that can be provided to a certain data stream may be too low for real-time multimedia services if all data streams get the same scheduling priority.
- **Dropped Packets**
 - The routers might fail to deliver (*drop*) some packets if they arrive when their buffers are already full. Some, none, or all of the packets might be dropped, depending on the state of the network, and it is impossible to determine what will happen in advance. The receiving application may ask for this information to be retransmitted, possibly causing severe delays in the overall transmission.
- **Error**
 - Sometimes packets are misdirected, or combined together, or corrupted, while *en route*. The receiver has to detect this and, just as if the packet was dropped, ask the sender to repeat itself.

 **DSNE** Digital Signage Network Expert

98

Quality of Service Standards

Internet Communications

- **Delay**
 - It might take a long time for a packet to reach its destination, because it gets held up in long queues, or takes a less direct route to avoid congestion. In some cases, excessive delay can render an application such as VoIP unusable.
- **Jitter**
 - Packets from the source will reach the destination with different delays. A packet's delay varies with its position in the queues of the routers along the path between source and destination and this position can vary unpredictably. This variation in delay is known as jitter and can seriously affect the quality of streaming audio and/or video.
- **Out-of-Order Delivery**
 - When a collection of related packets is routed through the Internet, different packets may take different routes, each resulting in a different delay. The result is that the packets arrive in a different order than they were sent. This problem requires special additional protocols responsible for rearranging out-of-order packets to an isochronous state once they reach their destination.
 - This is especially important for video and VoIP streams where quality is dramatically affected by both latency and lack of isochronicity.

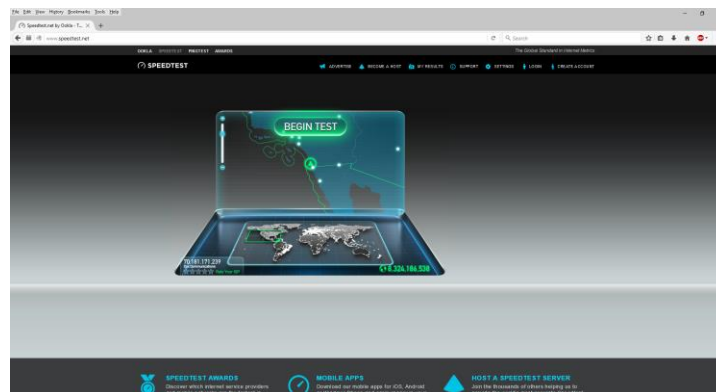
 **DSNE** Digital Signage Network Expert

99

Testing Internet Speeds

Internet Communications

- There are a number of high-quality speed testing online utilities. These utilities will test the upstream and downstream capabilities of an internet connection and report on how fast they are.



 **DSNE** Digital Signage Network Expert

100

Virtual Networking

VLANs and VPNs



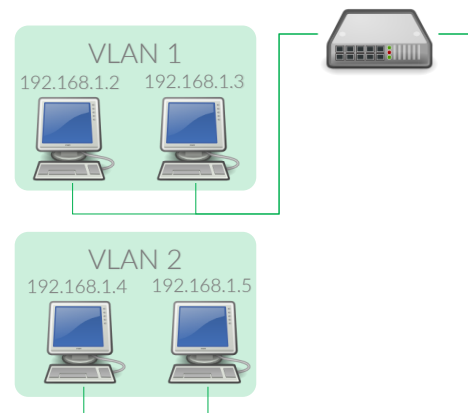
101

VLAN and VPN – Additional Ways to Connect

Virtual Networking

102

- A **VLAN (Virtual LAN)** is a way that network administrators can segregate traffic on their network.
- A VLAN requires managed switches capable of isolating groups of connected devices into their own network, with no access to other devices on the network.
- This is used for security purposes, and to limit the effect a system such as digital signage or streaming audio can have on the overall network.
- A VLAN has the same attributes as a physical LAN, but it allows for devices to be grouped together even if they are not located on the same network switch.
- Network reconfiguration can be done through software instead of physically relocating devices.



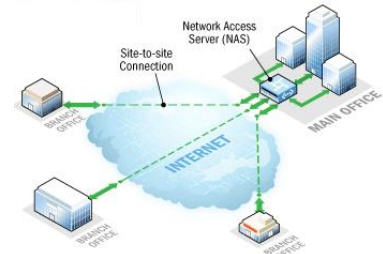
 DSNE Digital Signage Network Expert

102

VLAN and VPN – Additional Ways to Connect

Virtual Networking

- A **virtual private network (VPN)** is a virtual connection to a computer network that is layered on top of a separate network connection, typically the Internet.
- A VPN is typically used to allow someone at a remote site to connect to a LAN over the Internet in a secure manner, as if the user was directly connected to that LAN.
- The private nature of a VPN means that the data travelling over the VPN is not generally visible to, or is encapsulated from, the underlying network traffic.
- This is done with strong encryption, as VPN's are commonly deployed to be high-security tunnels for traffic.
- Similarly, the traffic within the VPN appears to the underlying network as just another traffic stream to be passed.
- This requires special software called a **VPN client** on the user's computer to create an encrypted stream of data that reaches out to a **VPN server** on the LAN and establishes a secure connection.



 **DSNE** Digital Signage Network Expert

103

Servers and Domains

Advanced Infrastructure

 **DSNE**
Digital Signage Network Expert

104

Server-Client and Peer-to-Peer Networking

Servers and Domains

- We can classify networks in terms of not just physical structure and protocols, but also sharing of resources.
- Client-server networks feature centralized **server** computers that store email, webpages, files and or applications for access by **clients**.
- On a **peer-to-peer** network, conversely, all computers tend to support the same functions.
- Client-server networks are much more common in business and peer-to-peer networks much more common in homes.



 **DSNE** Digital Signage Network Expert

105

Servers – More Than Just File Storage

Servers and Domains

- The word **server** is used quite broadly in information technology.
- Despite the many “server” branded products available (such as server editions of hardware, software and/or operating systems), in theory any device or application that shares a resource to one or more client devices is a server.
- To illustrate this, take the common example of file sharing. While the existence of files on a computer does not classify it as a server, the mechanism which shares these files to clients by the operating system is the server.
- Similarly, consider a web server application. This web server software can be run on any capable computer.
- For example, while a laptop or desktop is not typically known as a server, they can in these situations fulfill the role of one, and hence be labeled as one.
- It is in this case that the machine's purpose as a web server classifies it in general as a server.



 **DSNE** Digital Signage Network Expert

106

Servers – More Than Just File Storage

Servers and Domains

- In the hardware sense, the word server typically designates computer models intended for running software applications under the heavy demand of a network environment.
- In this client-server configuration one or more machines share information with each other with one acting as a host for the other.
- While nearly any personal computer is capable of acting as a network server, a dedicated server will contain features making it more suitable for production environments.
- These features may include faster or more CPUs, increased high-performance RAM, and typically more than one large hard drive.
- More obvious distinctions include marked redundancy in power supplies, network connections, and even the servers themselves.



 **DSNE** Digital Signage Network Expert

107

Servers – More Than Just File Storage

Servers and Domains

- **Hardware requirements for servers vary, depending on the server application.**
- Absolute CPU speed is not usually as critical to a server as it is to a desktop machine. Servers' duties to provide service to many users over a network lead to different requirements like fast network connections and high I/O throughput.
- Since servers are usually accessed over a network they may run in headless mode without a monitor or input device.
- Processes which are not needed for the server's function are not used. Many servers do not have a graphical user interface (GUI) as it is unnecessary and consumes resources that could be allocated elsewhere.
- Similarly, audio and USB interfaces may be omitted.
- Servers often run for long periods without interruption and availability must often be very high, making hardware reliability and durability extremely important.

 **DSNE** Digital Signage Network Expert

108

Servers – More Than Just File Storage

Servers and Domains

- Although servers can be built from commodity computer parts, mission-critical servers use specialized hardware with low failure rates in order to maximize uptime.
- For example, servers may incorporate faster, higher-capacity storage arrays, more cooling to help remove heat, and uninterruptible power supplies that ensure the servers continue to function in the event of a power failure.
- These components offer higher performance and reliability at a correspondingly higher price.
- Hardware redundancy - installing more than one instance of modules such as power supplies and hard drives arranged so that if one fails another is automatically available - is widely used.
- Servers are often rack-mounted and situated in server rooms for convenience and to restrict physical access for security.



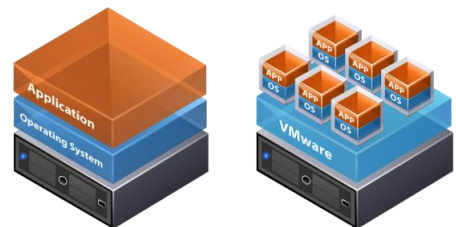
 **DSNE** Digital Signage Network Expert

109

Virtual Machines

Servers and Domains

- A server may not be physical hardware.
- Within IT today, many servers are created as **virtual machines**, or simulations of a distinct machine that runs as a process (often along with many other virtual machines) on a single set of physical hardware.
- This carries many advantages, including lower deployment costs (only one set of hardware to buy), flexibility (new machines can be started or “spun up” quickly based on pre-created images), and reliability (images of a virtual machine can be taken at any time, allowing for rapid repair if a failure occurs).
- Many companies are locating services into virtualized hardware within a few physical devices in a datacenter.



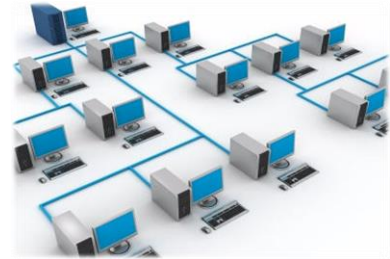
 **DSNE** Digital Signage Network Expert

110

Domains – Another Way to Network

Servers and Domains

- A **Windows Server domain** is a logical group of computers running versions of the Microsoft Windows operating system that share a central directory database and resources.
- This central database contains the user accounts and security information for the resources in that domain.
- Each person who uses computers within a domain receives his or her own unique account and assigned access to resources within the domain.
- In a domain, the directory database resides on computers that are configured as **domain controllers**.
- A domain controller is a server that manages all security-related aspects between user and domain interactions, centralizing security and administration.



 **DSNE** Digital Signage Network Expert

111

Domains – Another Way to Network

Servers and Domains

- A domain does not refer to a single location or specific type of network configuration.
- The computers in a domain can share physical proximity on a LAN or they can be located in different parts of the world. As long as they can communicate, their physical position is irrelevant.
- Computers can connect to a domain easily via LAN, or via WAN using a VPN connection.



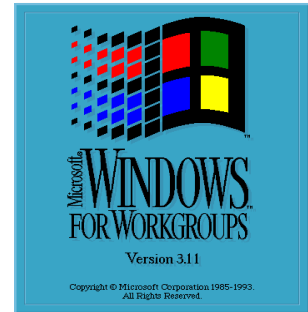
 **DSNE** Digital Signage Network Expert

112

Domains VS. Workgroups

Servers and Domains

- **Workgroups**, by contrast, are the other model for grouping computers running Windows in a networking environment.
- Workgroup computers are considered to be 'standalone' - i.e. there is no formal membership or authentication process formed by the workgroup.
- A workgroup does not have servers and clients, and as such, it represents the Peer-to-Peer (or Client-to-Client) networking model.
- Workgroups are considered difficult to manage beyond a modest number of clients, lack single sign on, scalability, resilience/disaster recovery functionality, and many security features.
- Workgroups are more suitable for small networks.



In Memoriam...

 **DSNE** Digital Signage Network Expert

113

Group Policies – Administrator Controlled Access

Servers and Domains

- **Group Policy** is a feature of Windows domains.
- Group Policy is a set of rules which control the working environment of user accounts and computer accounts, enforced on each computer by the domain controller.
- Group Policy provides the centralized management and configuration of operating systems, applications and users' settings.
- In other words, Group Policy in part controls what users can and can't do on a computer system.
- Although Group Policy is more often seen in use for enterprise environments, it is also common in schools, smaller businesses and other kinds of smaller organizations.
- Group Policy is often used to restrict certain actions that may pose potential security risks, for example: to block access to the Task Manager, restrict access to certain folders, disable the downloading of executable files and so on.



 **DSNE** Digital Signage Network Expert

114

Active Directory

Servers and Domains

- Active Directory (AD) is a database directory service Microsoft developed for Windows domain networks and is included in most Windows Server operating systems as a set of processes and services.
- Initially, Active Directory was only in charge of centralized domain management, but starting with Windows Server 2008, has become an umbrella name for a broad range of directory-based identity related services.
- The Active Directory Domain Services run on the domain controller and handles authentication and authorization of all users and computers.
- Active Directory also assigns and enforces security and group policies for all computers and installing and updating of software.
- Active directory provides DNS services inside the domain.
- Active Directory makes use of **Lightweight Directory Access Protocol (LDAP)** for accessing and maintaining distributed directory information services.



115

Dealing with Security Threats



116

Methodologies to Improve Security

Dealing with Security Threats

- **There are two theories in computer security that are 100% applicable in all cases:**
The first, **least privilege**, refers to a user being unable to make important changes to a computer without an administrator's sanction.
- Most MAC and *NIX users should be used to this concept, as they must authenticate as an administrator to make any changes to the system, even when logged in as an Administrator.
- Windows now implements similar concepts with **User Account Control**, which notifies users of changes, and requires approval. However, Windows accounts by default are created as Administrators, allowing full access. This should be changed in most cases.
- Second is the **reduced attack surface**. The fewer avenues of attack that are available, the more secure the system is overall.
- This means keeping your system up-to-date, with proper security software in place, enforcing group policies if possible, and leaving as few openings in system security as possible.

 **DSNE** Digital Signage Network Expert

117

Shields up! Firewall Protection

Dealing with Security Threats

- A firewall is the first line of defense for a network, between the outside world and the internal network.
- We have already discussed the role of a firewall in the network, and one should typically be deployed.
- Individual firewalls can also reside on computers inside the network, installed as a software application. One is even included as standard with Windows.
- Some traffic will need to be allowed through the firewall, but always be careful to not leave any more open ports than is necessary.



 **DSNE** Digital Signage Network Expert

118

Malware

Dealing with Security Threats

- **Malware**, short for **malicious software**, is software designed to infiltrate a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.
- The term **computer virus** is sometimes used as a catch-all phrase to include all types of malware, including true viruses.
- Software is considered malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, trojan horses, spyware, adware, ransomware, most rootkits, and other malicious and unwanted software.
- Malware is not the same as defective software, that is, software that has a legitimate purpose but contains harmful bugs.



 **DSNE** Digital Signage Network Expert

119

Good Medicine - Antivirus Software

Dealing with Security Threats

- **Antivirus software** is used to prevent, detect, and remove malware, including computer viruses, worms, and trojan horses. Such programs may also prevent and remove adware, spyware, and other forms of malware.
- A variety of strategies are typically employed. **Signature-based detection** involves searching for known malicious patterns in executable code. However, it is possible for a user to be infected with new malware for which no signature exists yet.
- To counter such so-called zero-day threats, **heuristics** can be used. One type of heuristic approach, generic signatures, can identify new viruses or variants of existing viruses by looking for known malicious code (or slight variations of such code) in files.
- Some antivirus software can also predict what a file will do if opened/run by emulating it in a sandbox and analyzing what it does to see if it performs any malicious actions. If it does, this could mean the file is malicious.



 **DSNE** Digital Signage Network Expert

120

Good Medicine - Antivirus Software

Dealing with Security Threats

- **However, no matter how useful antivirus software is, it can sometimes have drawbacks.**
- Antivirus software can degrade computer performance if it is not designed efficiently.
- Inexperienced users may have trouble understanding the prompts and decisions that antivirus software presents them with. An incorrect decision may lead to a security breach.
- If the antivirus software employs heuristic detection (of any kind), success depends on achieving the right balance between false positives and false negatives.
- False positives can be as destructive as false negatives. In one case, a faulty virus signature issued by Symantec mistakenly removed essential operating system files, leaving thousands of PCs unable to boot.
- Finally, antivirus software generally runs at the highly trusted kernel level of the operating system, creating a potential avenue of attack.
- In addition to the drawbacks mentioned above, the effectiveness of antivirus software has also been researched and debated. One study found that the detection success of major antivirus software dropped over a one-year period.

 **DSNE** Digital Signage Network Expert

121

Squashing Bugs – Antispyware Software

Dealing with Security Threats

- **As the spyware threat has worsened, a number of techniques have emerged to counteract it.**
- These include programs designed to remove or to block spyware, as well as various user practices which reduce the chance of getting spyware on a system.
- Anti-spyware programs can combat spyware in two ways:
- They can provide **real time protection** against the installation of spyware software on your computer. This type of spyware protection works the same way as that of anti-virus protection in that the anti-spyware software scans all incoming network data for spyware software and blocks any threats it comes across.
- Real-time protection from spyware works identically to real-time anti-virus protection: the software scans disk files at download time and blocks the activity of components known to represent spyware.
- In some cases, it may also intercept attempts to install start-up items or to modify browser settings.



 **DSNE** Digital Signage Network Expert

122

Squashing Bugs – Antispyware Software

Dealing with Security Threats

- **Anti-spyware software programs can be used solely for detection and removal of spyware software that has already been installed onto your computer.**
- This type of spyware protection is normally much easier to use and more popular. With this spyware protection software you can schedule weekly, daily, or monthly scans of your computer to detect and remove any spyware software that has been installed on your computer.
- This type of anti-spyware software scans the contents of the windows registry, operating system files, and installed programs on your computer and will provide a list of any threats found, allowing you to choose what you want to delete and what you want to keep.



 **DSNE** Digital Signage Network Expert

123

Wi-Fi Security

Dealing with Security Threats

- Since wireless networks are broadcast over a larger area, and any client that can receive the signal may connect, Wi-Fi security is essential.
- Wireless APs offer the ability to encrypt, or secure a connection using a password often known as a **passphrase**.
- This encryption can come in several levels:
- **WEP**
 - **Wired Equivalent Privacy (WEP)** is a security algorithm for IEEE 802.11 wireless networks.
 - Introduced as part of the original 802.11 standard, its intention was to provide data confidentiality comparable to that of a traditional wired network.
 - Using a stream cipher and a CRC (cyclic redundancy check), WEP encrypted wireless traffic using a key of either 10 or 26 hexadecimal digits.
 - WEP was at one time widely in use and was often the first security choice presented to users by router configuration tools, but today we understand that WEP is easily broken by simple, readily available software tools.

 **DSNE** Digital Signage Network Expert

124

Wi-Fi Security

Dealing with Security Threats

- **WPA**

- **Wi-Fi Protected Access (WPA)** is a security protocol and security certification program developed by the Wi-Fi Alliance to secure wireless computer networks.
- The Alliance defined these in response to serious weaknesses researchers had found in the previous system, WEP.
- **Temporal Key Integrity Protocol (TKIP)** was adopted for WPA. TKIP employs a per-packet key, meaning that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP.
- WPA also includes a message integrity check, which is designed to prevent an attacker from altering and resending data packets. This replaces the cyclic redundancy check (CRC) that was used by the WEP standard. CRC's main flaw was that it did not provide a sufficiently strong data integrity guarantee for the packets it handled.
- WPA also implemented the **PSK (Pre-Shared Key)** system, allowing a simple password of 8-63 ASCII characters to be used to secure the network.

 **DSNE** Digital Signage Network Expert

125

Wi-Fi Security

Dealing with Security Threats

- **WPA2**

- **WPA2 (Wi-Fi Protected Access 2)** is a Wi-Fi Alliance branded version of the 802.11i security standard, replacing WPA.
- The primary enhancement over WPA is the inclusion of the AES-CCMP algorithm as a mandatory feature. AES-CCMP is a much stronger encryption algorithm than previously used.



 **DSNE** Digital Signage Network Expert

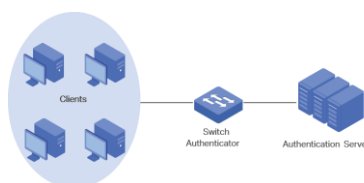
126

Wi-Fi Security

Dealing with Security Threats

- **802.1x Authentication**

- **802.1x Authentication** is an IEEE standard for secure network access. This is different from consumer style wireless networks in one major way – it has an authentication server called a **RADIUS server**.
- This checks a user's credentials to see if they are an active, approved member of the organization, and can be used to manage access to varying parts of the network (depending on network policies).
- A user will have to provide unique credentials to log in to this type of secure network for each use. Certificates can be used to provide permanent authentication, but they must be loaded by a device admin.



 **DSNE** Digital Signage Network Expert

127

Additional Wi-Fi Security Measures

Dealing with Security Threats

- **SSID hiding**

- A simple method to attempt to secure a wireless network is to hide the SSID. This provides very little protection against anything but the most casual intrusion efforts.

- **MAC ID filtering**

- One of the simplest techniques is to only allow access from known, pre-approved MAC addresses. Most wireless access points contain some type of MAC ID filtering. However, an attacker can simply sniff the MAC address of an authorized client and spoof this address.

- **Static IP addressing**

- Typical wireless access points provide IP addresses to clients via DHCP. Requiring clients to set their own addresses makes it more difficult for a casual or unsophisticated intruder to log onto the network, but provides little protection against a sophisticated attacker.

 **DSNE** Digital Signage Network Expert

128

Troubleshooting Principles

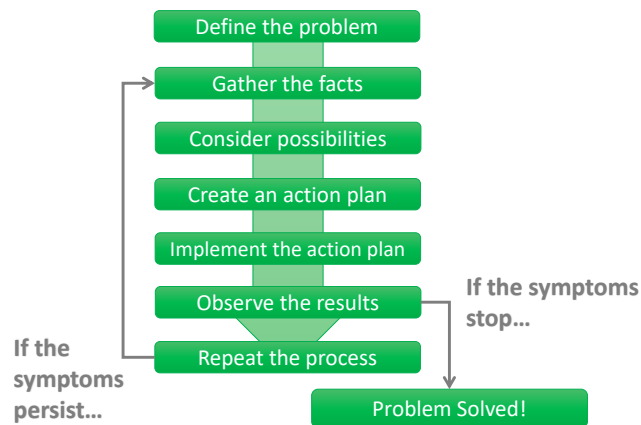


129

Troubleshooting Methodologies

Troubleshooting Principles

- Problem Solving Process



 DSNE Digital Signage Network Expert

130

Key Troubleshooting Principles

Troubleshooting Principles

- **First, DO NOT ASSUME!**
 - Nothing is beneath checking, including “is it plugged in?” or “is it turned on?”. Do not trust what you are being told, and do not assume that it is accurate. Always check for yourself whenever possible, from the most basic and obvious upward.
- **Second, TEST END TO END**
 - When approaching a system that does not work, there are a large number of variables present that must be ruled out.
 - Start at one end of the system, and work your way to the other side, checking all possibilities, and thus eliminating variables.
 - For example, a remote PC is not connecting to a server. Starting with the local system, verify that the server is accepting connections, check a local PC that is can see everything, and then move to the local router, the internet connection (local side), internet connection (far side), far side router, then the actual remote PC.
- **Third, adapt to USER INATTENTION**
 - Users are frequently willfully inattentive when it comes to using software, not reading pop ups, error messages, or consciously recognizing all aspects of an application.
 - This is why we hear “It crashed!” as a generic message, instead of getting feedback on a specific error.
 - You may need to poke at a topic to get useful information from an end user reporting issues!



131



ANY QUESTIONS?

“Successful people ask better questions, and as a result, they get better answers.”

Tony Robbins

132

Digital Signage Experts Group

Contact Us

Web:
www.dseg.org

Phone:
(442) 245 - 8332

Social:
@DSEG



Thank You!