Index

DIGISCENT

Being able to mechanically recreate one of the five senses, namely smell, has been in the works for quite some time now. A company called DigiScents believes they have the goods to revolutionize the way we think of smell. They have recently teamed up with Quest International, one of the world's leading fragrance, flavor and food ingredients manufacturers, with particular strengths in sensory design and consumer understanding. Together, they envision a vast array of new opportunities, mostly in they way they plan on making this new technology profitable.

Currently we are limited in the way we can experience things through our computer. We can see, hear, and to some extent touch what is presented on our monitors. However, no computer simulation can recreate a walk on the beach, or shopping in a bakery shop. Sure, you might be able to see and hear, but you miss out on the smell of the sea spray and the fresh baked bread. Well fear no longer. With the smell device you can smell all those things and then some.

The digitalization and broadcast of scent will enable consumers to send scented mail, smell's shop, watch scented DVDs, and play scented games. As you can imagine, there are many pluses to being able to smell those flowers or fragrances before you buy them. However, how willing are you to smell what it is really like in those first person shooter games? Do you really want to take simulated killing one step closer to being reality? Other than that, I'm all for smelling digital roses.

NET SCENTS

Imagine sending your significant other an e-card with not just the image but the smell of a dozen red roses. Or, how about treating your annoying cousin to both the vision and the odor of Patrick Ewing's socks after four quarters of posting up Tim Duncan.

Sounds like something out of a John Waters flick (anyone remember Odorama?). But scratch-n-sniff e-cards, Internet ads and video games will soon be reality with digital-scent technology from DigiScents, a privately held company in Oakland, Calif.

Here's how it works: A scent is digitized based on its molecular composition and its interaction with neuro-receptors in the brain. The result is a digital file that can be embedded into video games, MP3 files, e-mail, Flash animations and streaming media. The end user needs

DigiScent's smell, a computer accessory similar to a set of speakers, which synthesizes the smell from its palette of "primary odors" and blows scented air out at the user.

The smell unit isn't available yet?DigiScent expects to release it sometime in 2001. The company has been coy about pricing so far, saying only that Smell's retail price would be comparable to other computer accessories such as speakers. DigiScent has big plans for the technology, predicting it'll be a big deal in online advertising (the company already has a strategic relationship with Procter & Gamble). And DigiScent CEO Joel Bellenson says that interested food and beverage, household product and cosmetics companies have been sniffing around.

Meanwhile, DigiScent is launching Snortal, a scent-enabled portal where you can send scented e-mail, register your own smells and create Scent Tracks for your favorite movies and music. "We want to become the Napster of smell," says Bellenson.

DigiScent smell

Although at first sight this may appear to be the most bizarre of the new technologies reviewed here, in many respects it could turn out to be the most significant of all for Web merchants. Smell is one of our most important senses and is heavily relied on when making purchasing decisions. That's why shoe stores and bakeries go to great lengths to fill their stores with the smells of their products. If you're selling ?smelly? products such as perfumes, candles etc. then you should be able to significantly increase your sales by enabling shoppers to smell your products.

There are two main parts to the smell system, software and hardware. The software is named Scent Streams, and DigiScent have recently signed an agreement with Real Networks to allow this software to be auto-downloaded to their installed base of some 100 million RealPlayer systems. The resulting widespread availability of the Scent Streams software should go a long way to ensuring the success of the smell system.

The other part of the system is the smell Personal Scent Synthesizer, which is due to be launched at the end of this year. The synthesizer plugs in to either the serial or USB port of a computer and uses small,

replaceable scent cartridge (similar to inkjet cartridges) to generate scents by emitting one or more scents from a ?palette? of around 100.

No pricing information is available yet on the synthesizer, although DigiScents say they are planning to make it a ?very low cost? peripheral, similar in price to a computer speaker. Clearly, the success of the DigiScent system is totally dependent on how many synthesizers they can sell.

My gut feel is that novelty value alone should ensure healthy sales as long as they can get the price low enough.

Types of Networks

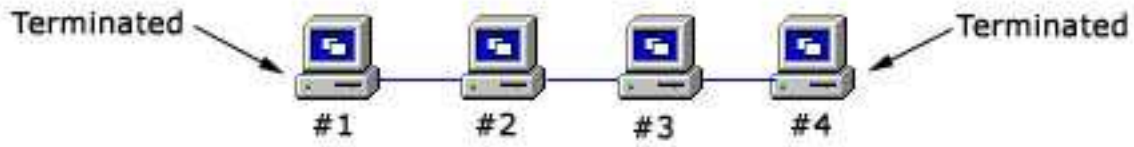
Peer to Peer - A peer to peer network is one in which lacks a dedicated server and every computer acts as both a client and a server. This is a good networking solution when there are 10 or less users that are in close proximity to each other. A peer to peer network can be a security nightmare, because the people setting permissions for shared resources will be users rather than administrators and the right people may not have access to the right resources. More importantly the wrong people may have access to the wrong resources, thus, this is only recommended in situations where security is not an issue.

Client/Server - This type of network is designed to support a large number of users and uses dedicated server/s to accomplish this. Clients log in to the server/s in order to run applications or obtain files. Security and permissions can be managed by 1 or more administrators which cuts down on network users medling with things that they shouldn't be. This type of network also allows for convenient backup services, reduces network traffic and provides a host of other services that comes with the network operating system(NOS).

Centralized - This is also a client/server based model that is most often seen in UNIX environments, but the clients are "dumb terminals". This means that the client may not have a floppy drive, hard disk or CDROM and all applications and processing occur on the server/s. As you can imagine, this requires fast and expensive server/s. Security is very high on this type of network.

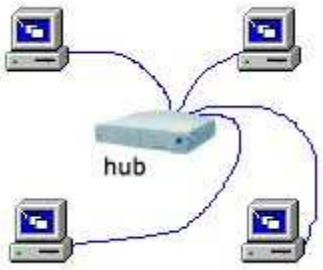
Network Topologies

Bus - This topology is an old one and essentially has each of the computers on the network daisy-chained to each other. This type of network is usually peer-to-peer and uses Thinnet (10base2) cabling. It is configured by connecting a "T-connector" to the network adapter and then connecting cables to the T-connectors on the computers on the right and left. At both ends of the chain, the network must be terminated with a 50 ohm impedance terminator. If a failure occurs with a host, it will prevent the other computers from communicating with each other. Missing terminators or terminators with an incorrect impedance will also cause problems.



As you can see if computer #1 sends a packet to computer #4, it must pass through computers #2 and #3, creating excess traffic.
ADVANTAGES: Cheap, simple to set up.
DISADVANTAGES: Excess network traffic, a failure may affect many users, problems are difficult to troubleshoot.

 Star - The star topology uses twisted pair (10baseT or 100baseT) cabling and requires that all devices are connected to a hub.



ADVANTAGES: centralized monitoring, failures do not affect others unless it is the hub, easy to modify.
DISADVANTAGES: If the hub fails then everything connected to it is down. This is like if you were to burn down the phone company's central office, then anyone connected to it wouldn't be able to make any phone calls.

Ring - The ring topology looks the same as the star, except that it uses special hubs and ethernet adapters. The ring topology is used with Token Ring networks.
ADVANTAGES: Equal access.
DISADVANTAGES: Difficult to troubleshoot, network changes affect many users, failures affect many users.
Hybrid - Hybrid topologies are combinations of the above and are common on very large networks. For example, a star bus network has hubs connected in a row (like a bus network) and has computers connected to each hub as in the star topology.

Mesh - In a true mesh topology every node has a connection to every other node in the network. A full mesh network can be very expensive, but provides redundancy in case of a failure between links.

Wireless - As the name implies, wireless networks allow computers to comunicate without the use of cables. IEEE 802.11b defines two pieces of equipment, a wireless station, which is usually a PC or a Laptop with a wireless network interface card (NIC), and an Access Point (AP),which acts as a bridge between the wireless stations and Distribution System (DS) or wired networks. An 802.11b wireless network adapter can operate in two modes, Ad-Hoc and Infrastructure. In infrastructure mode, all your traffic passes through a wireless ?access point?. In Ad-hoc mode your computers talk directly to each other and do not need an access point at all. 802.11b delivers data throughput of 11 Mbps.
ADVANTAGES: World-wide acceptance. Ranges over 150 feet. Freedom to move about and no cables (obvious).
DISADVANTAGES: Susceptible to interference from objects such as microwave ovens and cordless phones.

CABLING

The table below lists some of the various cable types.

Cable Type	Also Known As	Connector	Maximum Length	Speed
10Base5	RG-8 or RG-11, Thicknet coax	AUI/DIX	500 meters(1640 ft)	10 mbps
10Base2	RG-58, thinnet coax	BNC connector	185 meters(607 ft)	10 mbps
10BaseT	Cat 3, 4, 5 twisted pair	RJ-45	100 meters(328 ft)	10 mbps
100Base-TX	Cat 5 twisted pair	RJ-45	100 meters(328 ft)	100 mbps
100Base-FX	Fiber Optic	ST, SC	2 Kilometers(6562 feet)	200 mbps
1000Base-T - Gigabit Ethernet	CAT5/CAT5e	RJ-45	100 meters(328 ft)	1 gbps
802.11b	Wireless / WiFi	No cabling. Uses Access Point (AP) for connection	150+ feet	11 mbps

This next table lists the transmission speeds of the various cable types.

Transmission Medium	Transmission Speed
Thicknet	10mbps
Thinnet	10 mbps
cat 2 twisted pair	4 mbps
cat 3 twisted pair	10 mbps
cat 4 twisted pair	16 mbps
cat 5 twisted pair	1000 mbps

Fiber Optic	100 mbps - 1 gbps
802.11b	11 mbps

Miscellaneous Cable Info

 Shielded twisted pair (STP) differs from UTP in that it has a foil jacket that helps prevent crosstalk. Crosstalk is signal overflow from an adjacent wire.

 The 5-4-3 rule: this rule states that a 10base2 network can have 5 cable segments connected with 4 repeaters, but only 3 of these segments can be occupied by computers. There is also a maximum of 30 computers per segment.

 Thicknet cables are 0.5 inches thick and have a 50 ohm impedance.

 Thinnet cables are 0.25 inches thick and have a 50 ohm impedance.

 Plenum grade cabling is required if the cabling will be run between the ceiling and the next floor (this is called the plenum). Plenum grade cabling is resistant to fire and does not emit poisonous gasses when burned.

 Thicknet is often used as a backbone. A transceiver with a vampire tap penetrates the core of the cable. From the transceiver a DB-15 connector plugs into the AUI port on a given device.

 Fiber Optic cabling has an built in security as you can't intercept data as you can with other cable mediums.

Network Hardware

Below are some of the common hardware devices found on a network. NOTE: The higher the network device is in the OSI layer the more intelligent the device is.

- **Network Interface Card:** - A Network Interface Card, often abbreviated as NIC, is an expansion board you insert into a computer so the computer can be connected to a network. Most NICs are designed for a particular type of network, protocol and media, although some can serve multiple networks.
- **Hub:** - A hub is used to connect computers on an ethernet network.
- **Repeater:** - Boosts signals in order to allow a signal to travel farther and prevent attenuation. Attentuation is the degradation of a signal as it travels farther from its origination. Repeaters do not filter packets and will forward broadcasts. Both segments must use the same access

method, which means that you can't connect a token ring segment to an Ethernet segment. Repeaters can connect different cable types.

- **Bridge** - Functions the same as a repeater, but can also divide a network in order to reduce traffic problems. A bridge can also connect unlike network segments (ie. token ring and ethernet). Bridges create routing tables based on the source address. If the bridge can't find the source address it will forward the packets to all segments. Bridging methods:
  - Transparent - Only one bridge is used.
  - Source-Route - Bridging address tables are stored on each PC on the network
  - Spanning Tree - Prevents looping where there exists more than one path between segments
- **Switch** - A switch prevents traffic jams by ensuring that data goes straight from its origin to its proper destination, with no wandering in between. Switches remember the address of every node on the network, and anticipate where data needs to go. It only operates with the computers on the same LAN. It isn't smart enough to send data out to the internet, or across a WAN. These functions require a router.
- **Router** - A router is similar to a switch, but it can also connect different logical networks or subnets and enable traffic that is destined for the networks on the other side of the router to pass through. Routers can connect networks that use disimilar protocols. Routers also typically provide improved security functions over a switch. Unroutable protocols can't be fowarded.
- **Gateway** - Often used as a connection to a mainframe or the internet. Gateways enable communications between different protocols, data types and environments. This is achieved via protocol conversion, whereby the gateway strips the protocol stack off of the packet and adds the appropriate stack for the other side.
- **Modem** - The modem is a device that converts digital information to analog by MODulating it on the sending end and DEModulating the analog information into digital information at the receiving end. Most modern modems are internal, however, they can be internal or external. External modems are connected to the back of the system board via a RS-232 serial connection. Internal modems are installed in one of the motherboard's PCI or ISA expansion slots depending on the modem. The modem contains an RJ-11 connection that is used to plug in the telephone line. Modems have different transmission modes as follows:
  - Simplex - Signals can be passed in one direction only.
  - Half Duplex - Half duplex means that signals can be passed in either direction, but not in both simultaneously. Half-duplex modems can work in full-duplex mode.
  - Full Duplex - Full duplex means that signals can be passed in either

direction simultaneously.

Modems can also be classified by their speed which is measured by the BAUD rate. One baud is one electronic state change per second. Since a single state change can involve more than a single bit of data, the Bits Per Second(BPS) unit of measurement has replaced it as a better expression of data transmission speed. Common modem speeds are V.34 at 28.8 kbps, V.34+ at 33.6 kbps and V.90 at 56 Kbps.

- **ISDN Adapter** - ISDN service is an older, but still viable technology offered by phone companies in some parts of the U.S. ISDN requires an ISDN adapter instead of a modem, and a phone line with a special connection that allows it to send and receive digital signals.
- **CSU/DSU** - A CSU/DSU (Channel Service Unit / Data Service Unit) is a piece of equipment that connects a leased line from the telephone company to the customer's equipment (such as a router). Although CSU/DSU's look similar to modems, they are not modems, and they don't modulate or demodulate between analog and digital. All they really do is interface between a 56K, T1, or T3 line and serial interface (typically a V.35 connector) that connects to the router. Many newer routers have 56K or T1 CSU/DSUs build into them.
- **Wireless Access Point** - A Wireless Access Point is a radio frequency transceiver which allows your wireless devices to connect with your home network and to the internet. A wireless access point will support up to 32 wireless devices. The data rate through this wireless network is 11 MegaBits per second.
- **Proxy** - A proxy server acts as a middle-man between clients and the Internet providing security, administrative control, and caching services. When a user makes a request for an internet service and it passes filtering requirements, the proxy server looks in its local cache of previously downloaded web pages. If the item is found in cache, the proxy server forwards it to the client. This reduces bandwidth through the gateway. If the page is not in the cache, the proxy server uses Network Address Translation (NAT) to use one of its own IP addresses to request the page from the appropriate server.
- **Firewall** - Either a hardware or software entity that protects a network by stopping network traffic from passing through it. In most cases, a firewall is placed on the network to allow all internal traffic to leave the network (emails to the outside world, web access, etc.), but stop unwanted traffic from the outside world from entering the internal network.

OSI 7 Layer Model

The OSI networking model is divided into 7 layers. Each layer has a different responsibility, and all the layers work together to provide network data communication.

- **Physical** - The Physical layer is the specification for the hardware connection, the electronics, logic circuitry, and wiring that transmit the actual signal. It is only concerned with moving bits of data on and off the network medium. Most network problems occur at the Physical layer.
- **Data Link** - The Data Link layer is the interface between the upper "software" layers and the lower "hardware" Physical layer. One of its main tasks is to create and interpret different frame types based on the network type in use. The Data Link layer is divided into two sub-layers: the Media Access Control (MAC) sub-layer and the Logical Link Control (LLC) sub-layer.
  - LLC sub-layer starts maintains connections between devices (e.g. server - workstation).
  - MAC sub-layer enables multiple devices to share the same medium. MAC sub-layer maintains physical device (MAC) addresses for communicating locally (the MAC address of the nearest router is used to send information onto a WAN).
- **Network** - The Network layer addresses messages and translates logical addresses and names into physical addresses. It also manages data traffic and congestion involved in packet switching and routing. It enables the option of specifying a service address (sockets, ports) to point the data to the correct program on the destination computer.
- **Transport** - The Transport layer provides flow control, error handling, and is involved in correction of transmission/reception problems. It also breaks up large data files into smaller packets, combines small packets into larger ones for transmission, and reassembles incoming packets into the original sequence.
- **Session** - The Session layer handles security and name recognition to enable two applications on different computers to communicate over the network. Manages dialogs between computers by using simplex(rare), half-duplex or full-duplex. The phases involved in a session dialog are as follows: establishment, data-transfer and termination.
- **Presentation**- The Presentation layer determines data exchange formats and translates specific files from the Application layer format into a commonly recognized data format. It provides protocol conversion, data translation, encryption, character-set conversion, and graphics-command expansion.
- **Application** - The Application layer represents user applications, such as

software for file transfers, database access, and e-mail. It handles general network access, flow control, and error recovery. Provides a consistent neutral interface for software to access the network and advertises the computers resources to the network.

Protocols

Protocols are the special set of rules that end points use in a telecommunication connection when they communicate. These rules allow computers with dissimilar operating sytems, network topologies, hardware, etc. to communicate. Next is a description of some of the more common protocols:

- **TCP/IP** - TCP/IP is the protocol suite of the internet and will be covered in the next section.
- **IPX/SPX** - These protocols were developed by Novell and are/were used with Novell Netware. IPX is the fastest routable protocol and is not connection oriented. IPX addresses are up to 8 characters in hexadecimal format. SPX is connection oriented.
- **NetBeui** - Stands for "NetBIOS Extended User Interface". It is the standard protocol used by Microsoft's operating systems. It is NetBEUI that allows the "shares' between machines. In reference to the NetBIOS distinction, NetBIOS is the applications programming interface and NetBEUI is the transport protocol. NetBEUI is a non-routable protocol meaning it will not allow communication through a router.
- **Appletalk** - AppleTalk is the name given to the set of protocol and networking standards created by Apple Computer for use with the Macintosh family of computers. AppleTalk is routable and automatically handles such things as assigning of workstation and network addresses, message routing between networks, etc.

TCP/IP

TCP/IP Protocol Suite The TCP/IP protocol suite is made of many other

protocols that perform different functions. Below is a list of some of them:

- **TCP** - TCP breaks data into manageable packets and tracks information such as source and destination of packets. It is able to reroute packets and is responsible for guaranteed delivery of the data.
- **IP** - This is a connectionless protocol, which means that a session is not created before sending data. IP is responsible for addressing and routing of packets between computers. It does not guarantee delivery and does not give acknowledgement of packets that are lost or sent out of order as this is the responsibility of higher layer protocols such as TCP.
- **UDP** - A connectionless, datagram service that provides an unreliable, best-effort delivery.
- **ICMP** - Internet Control Message Protocol enables systems on a TCP/IP network to share status and error information such as with the use of PING and TRACERT utilities.
- **SMTP** - Used to reliably send and receive mail over the Internet.
- **FTP** - File transfer protocol is used for transferring files between remote systems. Must resolve host name to IP address to establish communication. It is connection oriented (i.e. verifies that packets reach destination).
- **TFTP** - Same as FTP but not connection oriented.
- **ARP** - provides IP-address to MAC address resolution for IP packets. A MAC address is your computer's unique hardware number and appears in the form 00-A0-F1-27-64-E1 (for example). Each computer stores an ARP cache of other computers ARP-IP combinations.
- **POP3** - Post Office Protocol. A POP3 mail server holds mail until the workstation is ready to receive it.
- **IMAP** - Like POP3, Internet Message Access Protocol is a standard protocol for accessing e-mail from your local server. IMAP (the latest version is IMAP4) is a client/server protocol in which e-mail is received and held for you by your Internet server.
- **TELNET** - Provides a virtual terminal or remote login across the network that is connection-based. The remote server must be running a Telnet service for clients to connect.
- **HTTP** - The Hypertext Transfer Protocol is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. It is the protocol controlling the transfer and addressing of HTTP requests and responses.
- **HTTPS** - Signifies that a web page is using the Secure Sockets Layer (SSL) protocol and is providing a secure connection. This is used for secure internet business transactions.
- **NTP** - Network Time Protocol is a protocol that is used to synchronize computer clock times in a network of computers.

- **SNMP** - Stands for Simple Network Management Protocol and is used for monitoring and status information on a network. SNMP can be used to monitor any device that is SNMP capable and this can include computers, printers, routers, mainframes, gateways and many more.

TCP/IP Ports

Ports are what an application uses when communicating between a client and server computer. Some common ports are:

- 21 FTP
- 23 TELNET
- 25 SMTP
- 69 TFTP
- 80 HTTP
- 110 POP3

TCP/IP Addressing

Every IP address can be broken down into 2 parts, the Network ID(netid) and the Host ID(hostid). All hosts on the same network must have the same netid. Each of these hosts must have a hostid that is unique in relation to the netid. IP addresses are divided into 4 octets with each having a maximum value of 255. We view IP addresses in decimal notation such as 124.35.62.181, but it is actually utilized as binary data.

IP addresses are divided into 3 classes as shown below:

Class	Range
A	1-126
B	128-191
C	192-223

NOTE: 127.x.x.x is reserved for loopback testing on the local system and is not used on live systems. The following address ranges are reserved for private networks:
10.0.0.0 - 10.254.254.254
172.16.0.0 - 172.31.254.254
192.168.0.0 - 192.168.254.254

IP addresses can be class A, B or C. Class A addresses are for networks with a large number of hosts. The first octet is the netid and the 3 remaining octets are the hostid. Class B addresses are used in medium to large networks with the first 2 octets making up the netid and the remaining 2 are the hostid. Class C is for smaller networks with the first 3 octets making up the netid and the last octet comprising the hostid. The

Network ID and the Host ID are determined by a subnet mask. The default subnet masks are as follows:

CLASS	DEFAULT SUBNET	# OF SUBNETS	# OF HOSTS PER SUBNET
Class A	255.0.0.0	126	16,777,214
Class B	255.255.0.0	16,384	65,534
Class C	255.255.255.0	2,097,152	254

NETBIOS

There are several different methods of resovling names to IP addresses. Before getting into the different methods, it is important to understand the role of NetBIOS. When talking about Netbios, we typically refer to the concept of Netbios name which is the name assigned to your computer. Netbios allows applications to talk to each other using protocols such as TCP/IP that support Netbios. Netbios is typically seen in other forms such as Netbeui and NetBT. These are the main functions that Netbios serves:

- Starting and stopping sessions.
- Name registration
- Session layer data transfer(reliable)
- Datagram data transfer(unreliable)
- Protocol driver and network adapter management functions.

NETBIOS Naming:

A Netbios name is either a unique name or a group name, the difference being that a unique name is used for communication with a specific process on a computer, whereas a group name is for communication with multiple clients. Netbios name resolution resolves a computer's Netbios name to an IP address. Microsoft offers several different ways to resolve Netbios names and each will be disscussed below.

- **Local Broadcast** - If the destination host is local, then first the Netbios name cache is checked and a broadcast is not sent. If it is not found here, then a name query broadcast is sent out that includes the destination Netbios name. Each computer that receives the broadcast checks to see if it belongs to the name requested. The computer that owns the name then uses ARP to determine the MAC address of the source host. Once obtained a name query response is sent. NOTE: Some routers do not

support the fowarding of these broadcasts as they use UDP ports 137 and 138.

- **NETBIOS Name Server** - When using a Netbios name server, the cache is checked first and if the name is not found the destination host's name is sent to the name server. After the name server resolves the name to an IP address, it is returned to the source host. When the source host receives the information it uses ARP to resolve the IP address of the destination host to it's MAC address. Microsoft uses WINS as a NETBIOS name server.
- **LMHOSTS File** - An lmhosts file is a text file that is used to manually configure Netbios names. In order to work, each entry in the lmhosts file must be unique, have a valid IP address for the Netbios name and be spelled correctly. On large networks configuring LMHOSTS files on all clients is not feasible, so these are not used much anymore.
- **Hosts File** - The hosts file is a little different than the lmhosts file in that it will resolve both local and remote names. If the host name can't be resolved and no other alternative name resolution processes are in place, the user will receive an error. Once the host name is parsed from the host file, ARP takes over and attempts to resolve the IP address to a MAC address. Like the lmhosts method, this is static name resolution.
- **DNS** - More on this later...

DNS

TCP/IP networks used to use hosts files to resolve IP addresses to host names or domain names. Networks began growing to the point where the administration and the traffic needed to maintain this file became unbearable and DNS was born. A DNS client(aka resolver) sends requests to the DNS nameserver which responds with the requested info, another server to query or a failure message. This process is very similar to calling information. You call them with a name, they check their database and give you the phone number. There are a variety of roles a nameserver can satisfy within the zone that they are responsible for:

- **Primary Nameserver** - Gathers DNS information from local files and is a focal point for adding hosts and domains.
- **Secondary Nameserver** - Gathers the data for its' zone(s) from another DNS server. Secondary nameservers provide redundancy, traffic on primary server and quicker access for locations that are remote in regards to the primary server.
- **Caching Only Nameserver** - These do not have a zone that they are

responsible for. Their databases only contain info that is received from resolutions that it has made since the server was last started.

Nameservers are distributed into tiers called domains.