Future of Home Networking

Tom Schmidt
Schmidt Consulting
5 February 2006
tom@tschmidtdotcom
http://www.tschmidt.com

Abstract

A decade ago computer networks were the province of Fortune 500 company IT departments. Today anyone can purchase a $50 router and set up a home network. The next decade will see continued advancement of wired and wireless networking and increased convergence of all electronic devices.

This paper looks at current trends and extrapolates likely changes over the next decade. As electronics becomes more capable and cheaper everything will be networked: from computers to light switches.

Today wired Ethernet is ubiquitous at low cost. Wireless Ethernet is also extremely popular because it facilitates mobility at the expense of speed and reliability. As Wireless becomes faster and more secure it will become the preferred interconnect means for most applications.

ZigBee is poised to facilitate an expansion of building automation because it eliminates need to hard wired intelligent devices and can be implemented at very low cost and power consumption.

Table of Contents

Home of the Future

Access to digital information is becoming as necessary for modern life as telephone and electricity. This paper examines technology trends in an effort to predict how residential networking infrastructure will evolve over the next decade.

Short History of Data Networking

A decade ago Local Area Networking (LAN) was the province of Fortune 500 IT shops. Ethernet/IEEE 802.3 was popular but IBM's Token Ring still commanded a large market. Ethernet operated at 10 Mbps and used RG59 coax to daisy chain multiple computers. Token Ring used a passive hub and spoke physical network at 16 Mbps. The new EIA/TIA 568 Unshielded Twisted Pair (UTP) structured wiring standards were taking hold and ultimately revolutionized how network cabling is installed.

Jump ahead to 2006 Fast Ethernet (100 Mbps) or Gigabit Ethernet (1,000 Mbps) is a commodity built into most computers. EIA/TIA 568 structured wiring is universal. Ethernet Switches have replaced Hubs eliminating collision domains and supporting full duplex connection between any pair of Ethernet hosts. Switches greatly improve LAN performance.

The various flavors of Wireless Ethernet IEEE802.11, marketed under the WiFi umbrella, free devices from the tyranny of wired networking. WiFi is slower then wired Ethernet but more then adequate for most purposes. Wifi began at 1 Mbps but is now available at 54 Mbps and work is in process for much greater speed. After a rough start on the security front Industry and IEEE developed effective WiFi cryptographic protection to protect over the air transmissions called WiFi Protected Access (WPA).

Interest in small business and home networks was primarily driven by explosive growth of the Internet in the mid nineties with the advent of the World Wide Web (WWW). The World Wide Web made the Internet much easier to use. The introduction of Netscape's web browser and search engines such as Digital's AltaVista made finding and displaying information much more convenient. Suddenly the PC, which until that time, had been used primarily as a tool for local applications and data sharing within a workgroup, became the primary means to obtain information from distant servers via the Internet.

Internet standards such as Network Address Translation (NAT) and private addresses (RFC 1918) made it easy to link a LAN to the Internet. Plug and play enhancements and mass market availability of network components means anyone, willing to invest a little time to understand basic networking technology, is able to build an Internet connected home network. Truly a remarkable achievement in 10 short years.

The new Power over Ethernet (PoE) specification eliminates need for AC power at each Ethernet device and facilitates battery backup during power outages. A single Uninterruptible Power Supply (UPS) is able to maintain power to the entire network during commercial power outages.

Network speed used to be limited and very expensive. Economists call this a scarce resource. Telephony engineers, over the last hundred years, designed incredible systems tuned to extract maximum possible carrying capacity from limited and expensive resources. In the 21st Century the situation is much different. Just as the microprocessor ushered in the era of cheap computer cycles changes in technology mean network performance is no longer a scarce commodity but available in abundance. While more is better we are rapidly approaching the day when network speed is "good enough" for all but the most demanding user. The ability to transport data is no longer a limiting factor. Lets take a quick look at performance requirements:

Speed	Application
0.064 Mbps	- DS-0 Toll quality telephone voice (each direction)
0.128 Mbps	- MP3 compression near CD quality audio
1.400 Mbps	- Raw CD quality audio
1.544 Mbps	- T1 (Full-Duplex)
3.000 Mbps	- MPEG2 Compressed NTSC standard definition TV
10.000 Mbps	- Ethernet (Half or Full duplex)
11.000Mbps	- WiFi 802.11b
13.000 Mbps	- Transfer 100 MByte file in 1 minute
19.250 Mbps	- MPEG2 Compressed HDTV
44.736 Mbps	- T3 (Full Duplex)
54.000 Mbps	- WiFi 802.11a & 11g
54.000 Mbps	- Download SDTV movie in 5 min (3Mbps x 90 min)
100.000 Mbps	- Fast Ethernet (Full or Half Duplex)
142.200 Mbps	- Raw NTSC SDTV
250.000 Mbps	- WiFi 802.11n (in development)
360.000 Mbps	- Download HDTV movie in 5 min (20 Mbps x 90 min)
500.000 Mbps	- Ultra Wide Band radio (in development)
1000.000 Mbps	- Gig Ethernet (Full Duplex)
1056.000 Mbps	- PCI 32-bit 33MHz (ignores arbitration overhead HDX)
1244.000 Mbps	- OC-24 (Full Duplex)
1485.000 Mbps	- Raw HDTV
10000.000 Mbps	-10 Gig Ethernet and OC-192 (Full Duplex)

The chart shows wired Ethernet is more then adequate for just about any use. Wireless performance lags Wired so it may be a limiting factor. Wireless is a shared medium and vulnerable to factors that reduce overall speed. Due to the nature of over the air communication performance of WiFi is limited to about half peak speed. For example IEEE 801.11a, 54 Mbps is about equivalent to wired Ethernet operating at about 27 Mbps HDX.

If we assume the most demanding use of home networks will be watching HDTV video each device that renders video needs a connection of at least 20 Mbps. Servers and other devices that need to simultaneously support multiple streams obviously require a faster connection.

Wide Area Networks (WAN) are not as fast as the LAN but there has been impressive progress over the last few years. Many residential customers are able to obtain multi-megabit service. Fiber to the Premise (FTTP) promises virtually unlimited First-Mile speed.

Speed, Latency and Jitter

Often overlooked in the quest for speed is the problem of latency. The Internet was designed for data traffic that is very tolerant of latency. For example if a file transfer or print job is delayed a second due to network congestion no one will likely notice. As packet networks are used to deliver real-time and streaming media latency management is becoming critical.

When playing streaming media it is common practice to delay playback and capture incoming data to an elastic buffer. The output of the buffer is used to drive the payback engine. The size of the buffer determines how much latency can be tolerated. As long as the stream is not delayed more then the size of the buffer playback is unaffected. This technique works well for unidirectional flows such as TV and radio but cannot be used for telephony.

As the table shows telephony is not very demanding of network data rate. It is however very sensitive to latency. Telephone is a real time full duplex exchange. That means tricks used with unidirectional stream flows cannot be used to hide network latency. If round trip time exceed about 250 ms (1/4 second) normal conversation becomes difficult. Network design must address both delivery speed and control latency. Our situation is much simpler then the Telephony engineer of past. In our case the network, in general, has plenty of bandwidth. What we need is a mechanism to give preferential treatment to a limited amount of critical traffic that will never be more then a small fraction of total.

Latency is also critical for multi channel sound. Sound travels about a foot per millisecond. A foot offset occurs to the stereo image if one channel of a multi channel sound system is delayed a millisecond. The IEEE Residential Study Group is investigating feasibility of reducing Ethernet LAN jitter to allow applications, such as multiple speakers to utilize Ethernet for transport.

File transfer protocols are designed to tolerate errors and request retransmission of incorrect data. Streaming protocols do not have this luxury. If data is received in error, there is not enough time to perform a retransmission. Overall error rate must be low and application address the effect of occasional error.

Quality of Service

Quality of Service (QoS) metrics work on the premise that some traffic is more valuable then others. Currently all traffic on the Internet is carried as best effort. When a packet arrives at a router or switch it waits until all previous packets have been forwarded. QoS

mechanisms add a priority field to each packet. As packets arrive the switch or router evaluates the priority field. Higher priority packets move to the head of the queue.

This is a simply mechanism but it brings with it a host of problems. The most important is who gets to set priority. Obviously it is to the advantage of each application to set priority to the highest possible level. If all applications request the highest priority it is the same as having no priority the "tragedy the commons." QoS potentially affects Internet governance and first-mile access. ISPs may use QoS to enhance service to business partners and disadvantage others.

For residential customers LAN latency will not be a major issue due to availability of Gig Ethernet. The WAN interface will likely remain a potential point of congestion requiring access router manage and prioritize upload traffic and ISP do same for download.

Security

Wireless networks create severe security concerns. With a wired network an attacker must "physically plug" into the network. The situation is much different with Wireless. An attacker located hundreds of feet from the network can easily observe traffic and potentially inject malicious traffic onto the LAN.

IEEE 802.11 WiFi anticipated this and created a security mechanism call Wireless Equivalent Privacy (WEP). Unfortunately WEP was found to be deeply flawed and has been replaced with WiFi Protected Access (WPA). WPA provides much better authentication and privacy but is still in the early stage of deployment.

Ultra Wide Band

An interesting new wireless development is Ultra Wideband. This technology provides fantastically high throughput over distances of a few meters. At first one may wonder what value this technology might have? To see one only has to look at the back of a stack of A/V components. UWB has the potential to eliminate inter component wiring.

If the technology works as advertised it will dramatically ease configuration of A/V systems be eliminating all but power wiring. Typical home theater will consist of number of AV components interconnected by UWB and linked to home network by wired Ethernet or WiFi.

Future Proofing

I'm often asked about future proofing a home network – running fiber etc. The people asking the question tend to do linear extrapolations of what is being done today three isolated networks: Analog Phone, RF TV, and wired Ethernet. My advice is the future is extremely difficult to predict. Customers have shown a profound preference for mobility and have been willing to trade off quality and reliability to get it. The cellular phone market is a dramatic example.

This tells us as WiFi improves it will likely become the preferred local network connection. Wired Ethernet is by no means going away. But one needs to rethink the notion of spending several thousand dollars wiring residences with separate POTS/CATV/Data jacks at multiple locations in each room and expecting those decision to be relevant a couple of decades in the future. Where performance is king and mobility is not an issue wired Ethernet will remain dominate. However in many locations the allure of untethered connectivity will carry the day. As this paper was being written it was announced that for the first time laptop sales exceeded desktop PC sales.

How will next generation Access Point address these limitations? New standards will deliver more bits per second from each Hertz of RF bandwidth. Governments will discover the value of these unlicensed radios and allocate more RF spectrum increasing number of channels and/or channel width. Clever vendors will drastically reduce Access Point cost and develop software to facilitate rapid roaming between AP's for Voice over IP. As Access Point cost comes down they will be distributed like candy throughout the home.

As APs become ubiquitous they become a convenient device to add secondary functions. In the future a WiFi Access Point may include a ZigBee radio to coordinate building automation, temperature sensor, fire and smoke detector, room occupancy detector, hazardous material detection, etc. The sky is the limit.

The best approach to future proofing is to ignore technical details or trying to guess what sort of "wire" will be needed over the lifetime of the home. Rather install empty conduits from central wiring closet to various strategic locations throughout the residence. This approach provides maximum flexibility at lowest cost. When I built our home in the early 1980s I build a wire chase from basement to attic. Twenty-five years later it is full of wires I had no idea I needed back then,

Broadband Internet Access

The US FCC defines broadband as Internet access over 200 kbps in either direction. Basically this excludes dialup and ISDN but everything else qualifies as broadband. Until a few years ago residential users had to be content with dialup. Demand for better Internet access created fierce competition to deliver faster first-mile access at low cost. Multimegabit access is now available to many households for nominal cost. Broadband access of some sort is available in all industrialized countries for a large portion of the population.

How much speed is needed will obviously depend on how the connection is used. If activity is limited to browsing the web then a megabit or so is more then adequate. If the need is to run a popular multimedia web site then much more is needed. If the desire is to support IPTV HDTV then 20 Mbps or so is required for each stream.

VoIP and multiplayer game require QoS to minimize latency for these time sensitive applications.

Telephony - POTS vs VoIP vs Cellular

Phone users have dramatically shown they are willing to trade off cost and reliability for the benefits of mobility. Many people, especially younger customers, no longer even have a wired phone. If we combine the advantage of Voice over IP with the desire for mobility we have a very interesting concept, the multifunction Cellular/WiFi handset. When the phone is in range of valid WiFi network voice calls are transported over the Internet. When out of range the Cellular provider handles the call normally. This bimodal configuration results in a number of significant advantages for everyone.

1. Reduced pressure for additional cell towers. If home is in a cellular dead zone – no problem – call is transported over customer's WiFi connection

2. Reduces cellular capital cost – data can often be transported over the customer's network rather then expensive cell sites.

3. Single phone number regardless of how call is transported. No more work #, home #, cell #, etc.

4. Simplified integrated messaging and phone management. Fantastic integration with Internet applications.

5. Huge boon to corporate customers. Company assigns an employee a mobile phone. When phone is in range of corporate WiFi network calls are routed internally – no per minute changes. When caller is out of range works like standard cellular phone. If employee telecommutes WiFi is used to connect to the corporate network over an Internet. Same advanced PBX features as in the office at low cost. If employee goes to any corporate site call can be transported by internal corporate network. For many employees no need to even provide a costly wired desk phone.

6. Converged network, no longer necessary to provide separate phone and data network.

Latency is the Achilles heel of VoIP. The problem facing VoIP designers is very different then the original Telephone engineers. Telephone engineers had to deal with very expensive low bandwidth channels. That is not the case today, the pipes carrying Internet traffic have incredible capability, and voice is only a small fraction of total traffic. This allows a simple mechanism to give voice traffic priority. Identifying high priority voice packets allow routers to give them priority and forward them ahead of other traffic. This elegant mechanism does raise some difficult issues. How does one enforce fairness? If all

traffic is marked as high priority then the system breaks down. The notion of having some packets being more valuable then others breaks the egalitarian paradyne of the Internet where all packets are treated equally. It also open the door to ISPs creating tied services, giving preferred service to some packets at the expense of the other.

Television – Analog RF vs Digital RF vs IPTV

Broadcast and Cable TV service is resource constrained. In the case of Broadcast TV – by FCC allocated VHF/UHF channels, Cable is limited by the capacity of the transmission network – typically 100 - 150 channels. This scarcity is why Television and Radio have evolved as a one-to-many broadcast network. Given the technology available at the time it was not feasible to provide a unique stream to each customer. Mass media is the mass media due to technology limitations.

Since the invention of the printing press authors have been dependant on middlemen to publish and distribute their work. This led to the creation of the so-called mainstream media that controls distribution between artist and patron. In many cases middlemen who control distribution have become more powerful then the people whom actually create the works being distributed.

The Internet is causing tremendous change in the way artistic works are distributed. Prior to the Internet the distribution channel between artist and patron was difficult and capital intensive. The transition is ongoing with legacy companies desperately attempting to figure out how to exploit this new media without fundamentally changing their business model. It will likely be several more years before technical and business aspects solidify.

The long term impact on Broadband and home networking is still evolving. The media industry is working hard to force hardware and software vendors to incorporate Digital Rights Management (DRM) schemes. If this is successful end users will have circumscribed ability to use, transport, and store professionally generated content. Implementation of DRM may require government approval of hardware and software before it can be sold to end-users.

Internet technology theoretically enables anyone to set up shop as a TV or radio "station" and send real-time or non real time programs to customers. Emulating the broadcast one-to-many model requires a technique called multicast. This technology and business model is still being worked out but it allows a single copy of a program to be sent to many customers thus conserving bandwidth and greatly reducing cost.

In the future going to the library means using a computer or TV to retrieve a specific work from a catalog of potentially millions of items. The selected work is delivered directly to the patron's TV or computer. Video on Demand (VoD) makes tremendous demands on content server farm and the distribution network. However: the promise is incredible – retrieve any printed, video, or audio work whenever you want wherever you are.

The wired home network can easily meet these technical challenges. WiFi is still a little short on capacity and being a shared medium needs to address prioritizing issues to insure non critical tasks do not unduly interfere with high priority tasks. The difficulty is with the Wide Area Network (WAN). First-mile access bandwidth must improve by a couple of orders of magnitude to deliver true video on demand. IPTV convergence eliminates the need for a separate network to distribute programs. TV is just another packet to the Internet.

Artistic Expression

The Internet was designed as a transparent end-to-end network. As residential connection speed increases it opens the door to all sorts of exciting possibilities well beyond the notion of Internet as a digital replacement for legacy Broadcast and Cable TV networks.

Low cost direct per to person communication combined with low cost creative tools will revolutionize artistic expression and the relationship between artist and patron. No longer will artists be dependant on middlemen for creation and distribution.

The future should see a burgeoning assortment of niche sites dedicated to every conceivable interest. Regardless of how unique the broad reach of the Internet means the site is accessible to worldwide population of like minded individuals.

Collaboration

The same changes that enhance artistic expression will facilitate collaboration. Community of interest will be driven by group dynamics that have nothing to do with geographical location.

Collaboration is not necessarily demanding of the network, it all depends of what the group is doing. Editing a text document could probably be done over dialup, editing a multimedia production demands tremendous network resources.

Telecommuting

As jobs become ever more information centric the location where the task is performed becomes less important. Many companies have embraced telecommuting. Advances in technology will make it easier and less costly to remote the “office” environment to anywhere the employee wants to work. High speed First-Mile access delivers the same user experience as if the employee was physically in the office. Virtual Private Network (VPN) provides secure remote access to the corporate site. Voice over IP (VoIP) enables the same corporate telephone features to be remoted without need for hardwired circuits or dedicated facilities.

VPNs face a number of challenges when used with home networks. Network Address Translation (NAT) is often used to allow a single ISP assigned IP address to be shared by

more then one computer. Unfortunately NAT is very hostile to IPsec VPN. Most vendors have implemented numerous NAT work around, but NAT does impact the protection available with IPsec.

The most secure VPN to an employee's location is a tunnel. The VPN client directs all traffic to the corporate LAN. The down side of this configuration is performance and privacy. All traffic has be to encrypted and sent to the corporate LAN whether or not that is the ultimate destination. This means even personal traffic, not destined for work, transits the corporate network. An alternative is a split-tunnel. A Split-tunnel only carries traffic destined for the corporate LAN. Everything else uses the local Internet connection as usual. This solves the privacy issue but IT departments are loath to implement split-tunnel for security reasons. If the employee's machine is compromised the attacker can use it to relay directly to the corporate LAN.

Most residential broadband accounts are highly asymeritic; download is much faster then upload. This was done for both business and technical reasons. Telecommuting tends to be very demanding of upload performance. Documents and databases are downloaded, modified, and then uploaded. Some ISP have even gone so far at to prohibit VPNs on residential accounts stating this is a "business use" of the account.

Media Server

As our lives revolve ever more with computers and digital data storing and managing this vast amount of data becomes a challenge. I'm always somewhat chagrined I can use Google to find information from millions of web sites faster then a file I created on my own computer yesterday.

Who manages this data is still a question. Will average users want the responsibility of running their own redundant file server and backing up important data or is this something they would entrust to a third party? If so what is an attractive price point?

Archiving digital data is a problem being faced by librarians today. Will information created today be accessible decades from now when the application used to create, modify and view that data are long obsolete and perhaps the company out of business?

Publishing

Personal web servers are becoming very popular. As the tools to create original works improve more and more people will feel compelled to "publish" what they create. Much will be uninteresting – except perhaps to immediate family. But among this great outpouring will be hugely important works – that could not have happened without this technology.

Setting up a hosted server is one option; this is relatively cheap and easy today. Better broadband performance allows the server be moved in home saving a little money and giving the user more and better control over it.

As home networks and building automation become more common there will be a need to access the home remotely. In this case we are really talking about publishing to ourselves, perhaps only to immediate family members. Remote access requires an always-on connection – no connection means no access. It requires a security scheme to limit whom and to what the remote user has access. This is especially difficult because the remote user may be connecting from and untrustworthy computer – say an Internet kiosk.

The other technical challenge is the need to funnel connectivity through a single portal. Residential ISPs typically provide a single IP address. This poses a challenge for remote access if access to more then one computer is desired.

Building Automation

Engineers and press have been predicting for years that smart homes were just around the corner. Commercial buildings use building automation extensively, primarily for HVAC Heating Ventilating Air Condition and energy management. There are a number of building automation standards however automation typically required hardwired proprietary sensor and controllers. Because manufactures focused on commercial and industrial buildings cost tends to be high.

It is interesting to compare building automation to computer networking. The direct approach to building did not materialize, during this time Ethernet went through several iterations, as did computers. Suddenly having an isolated computer did not make sense. Much of what one needed was located elsewhere. During the time remote access was becoming more valuable the cost of implementing a LAN was dramatically reduced. This resulted in explosive growth of small business and residential LANs. When I installed a home LAN in 1998 residential LANs were still a rarity and one needed a fair amount of technical expertise to pull all the pieces together. Some ISP actually prohibited home LAN in their contracts. Today almost anyone with more then one computer can go to a computer store, pick up a router and set up a simple wired or wireless LAN in a few hours. The same transformation is needed in the building automation market. The answer may be ZigBee.

ZigBee/IEEE 802.3.15 is a low power radio technology optimized for sensor command and control networks. The main advantage of wireless is installation cost. Being wireless all one need do is purchase a device and mount it. No wiring except perhaps plugging it non-battery powered devices. ZigBee promises multi year battery life. Being a radio technology the same device and protocol can be used in either in either a fixed or portable mode, reducing development cost.

Mesh networking is not part of ZigBee but it will be an important technology for successful deployment. Over the air is a formidable medium. Lots of interference sources, potential eavesdropping, low power budgets. Without mesh the transmitter must have a clear path the receiver under all conditions for reliable communication. In a mesh

network rather then having to connect directly to a distant receiver the transmitter only needs to connect to the nearest router. The router forwards packets to the next router, and so forth until they finally arrives at the destination. Reducing distance between sender and receiver has a number of benefits. Transmit power is greatly reduced. Impact of noise sources is reduced and routers are able to route around noise sources. Reducing power leads to spatial frequency reuse. This increases overall performance since throughput of the entire network is improved. This works much the same a cellular network. Individual cell do not interfere with one another allowing the same channels to be reused.

Once this technology matures building automation cost will be greatly reduced. Numerous sensors such as occupancy, intrusion, environmental quality, and energy management can be installed for little more then the cost of the sensor.

The other critical aspect is a unified software infrastructure allowing end user to easily mix and match devices and software to accomplish the desired task. Much development work is going into creating robust device models to accomplish this.

Remote Management

Remote management is another area ripe for explosive growth. Setting up and managing a home network is getting easier but it is still a significant task requiring mastery of arcane jargon. The difficult business issue is to be able to deliver this service at a price point high enough to be profitable while being low enough to be attractive to potential customers.

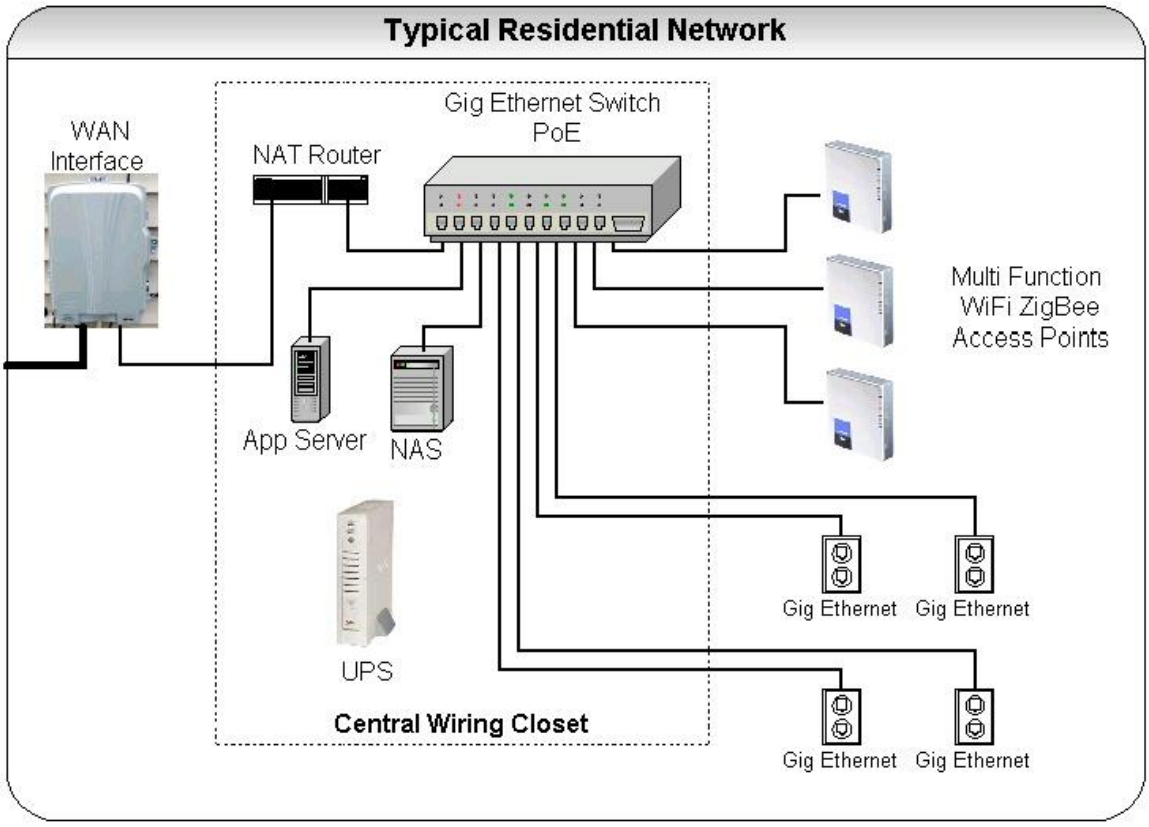
Backup Power

There is much discussion about whether or not the Internet is a necessity. As access to digital data becomes ever more tightly integrated with or day-to-day experience losing Internet access due to power failure becomes very disruptive.

Uninterruptible Power Supplies (UPS) have been available for years. A UPS consists of a standby power source, typically a battery, an inverter to convert battery voltage to standard AC power and a power supply to recharge the battery when commercial power is restored. Backup power needs to be delivered where it is needed. This second task has become much easier with the advent of Power over Ethernet (PoE). The same cable that transports Ethernet data can also be used to deliver about 13 Watts to each endpoint. This makes it much easier to deliver emergency power, as a single UPS in the wiring closet is able to power the entire network.

Putting it Together – Future Home Network

Lets pull everything together and identify what is needed for home network of the future.



The first-mile access provider is responsible for installing and configuring a Network Interface Device: typically a modem or in the case of FTTP an Optical Network Termination (ONT). The customer side uses a standard UTP Ethernet port to connect to customer premise equipment (CPE).

The WAN connection is feed to a NAT router. The router manages the Wide Area Network (WAN) connection and uses Network Address Translation (NAT) to allow an unlimited number of devices to share a single physical connection and IP address. The router often provides other services such as firewall, DMZ, SysLogging and Dynamic DNS update service and Quality of Service (QoS) upload management.

The Router's LAN port is fed to a multiport Gig Ethernet Switch. The Switch creates the LAN and allows Ethernet (10 Mbps) Fast Ethernet (100 Mbps) and Gig Ethernet (1,000 Mbps) NIC to interoperate. The Switch includes Power over Ethernet (PoE) enabling low power devices (~15W) to be powered directly from UTP Ethernet cable eliminating the need for direct AC power connection and allowing a centralized UPS to maintain power to all critical devices during power failure.

Network Attached Storage (NAS) is a local file server. This resource is used to backup data on individual PCs and for audio and video media storage.

The Application Server implements various applications such as managing multiple Access Points, providing secure remote access and converting ZigBee building automation data into Web based format for use by non ZigBee TCP/IP devices. This is really a catchall device for common services that need to be very reliable and operate during power failure.

Access Points convert wired Ethernet to WiFi and ZigBee radio. Access Points are a logical place to incorporate other sensors such as fire and smoke, temperature, occupancy, and environmental quality.

Non-mobile devices with well defined locations benefit from wired Ethernet. Wired Ethernet is faster and more reliable then wireless at the expense of requiring an outlet wherever it is needed.

Lastly an Uninterruptible Power Supply (UPS) maintains critical system operation during power failure.

What's Still Needed

QoS through the switch and more critically the NAT router is needed to insure high priority traffic gets priority. The ISP needs to support QoS so critical packets are not delayed as they traverse the ISP network.

Most residential WiFi equipment is built into the broadband router. Router location is typically not the best place to locate an Access Point and multiple Access Points are needed for high reliability coverage. Centralized Access Point coordination allows rapid handoff from one AP to another and enables intelligent handoff between APs for better load balancing. Centralized support is often used for large installations: cost and ease of use needs to improve to bring this to the home market.

Using WiFi to deliver Telephony has great potential but is still in its infancy. Combining WiFi and Cellular benefits both customers and Wireless carriers.

ZigBee building automation and mesh networks are still an emerging technology.

Network Attached Storage (NAS) has been successful in the commercial space. Network storage for home network requires low cost robust hardware, easy to use backup and management software.

Power over Ethernet has been wildly successful. However it is a relatively new technology. It will take a while to bring a broad range of devices to market.

Digital Convergence has been discussed for years. The advent of high-speed First-Mile Internet access and capable residential networking provides the infrastructure for application developers to move forward. Just as the last decade saw the creation of new companies and services so should the next.

Remote access to residential networks is still a rarity. A workable solution is needed that allows remote access from untrustworthy workstations without the need for additional software. NAT makes remote access more difficult since traditional VPN's may experience private network address collisions. The solution will need to be some sort of SSL (TLS) perhaps in conjunction with customer's cell phone to provide authentication and remote access without the need for remote device to be either trustworthy or run special software.

Home entertainment represents a complex dynamic between traditional media companies and the capability of new technology. Technology improvements drastically reduce the cost of distribution and undermine the value of content aggregators. Incumbents have been reluctant to create new business models that embrace technology change, instead are focused on crippling it to preserve their legacy business value. The various Digital Rights Management (DRM) mechanisms proposed so far have turned out to be unworkable and dramatically limit how customers are able to use lawfully purchased content.

Ultra Wide Band (UWB), once the jockeying for position is addressed, will eliminate the need to physically interconnect stackable devices. UWB coupled with plug and play device software will go a long way to make these systems easier to use and banish once and for all time the coffee table full of component remotes. Instead of a complex rats nest of home theater interconnect cabling interconnect will be wireless reducing wiring to a few power cables.

Lastly we need experts to design, install and manage these complex systems at a price point that makes sense for the Management Company and end user. No matter how easy it becomes to install only a small percentage of customer will be willing to invest the effort to obtain the specialize skills needed to successfully install and manage a residential network.

Closing Thoughts

The future of residential networking and home automation is bright. The Internet and advances in semiconductor technology represent tremendous advancement in personal communication. Never before has it been so easy to reach out and touch someone no matter where they are.