Journal of Electrical Engineering and Electronic Technology

Editorial A SCITECHNOL JOURNAL

Importance of wireless network management

Christophe Dunand

Nanjing University of Posts and Telecommunications

***Corresponding author:** G.Prakash Department of Electronics and Communication, Bharath university, Chennai, India, E-mail: kanags89@gmail.com

Received date: December 08, 2021; **Accepted date:** December 19, 2021; **Published date:** December 27, 2021

Editoral Note

A broadband Internet connection is a high-speed Internet connection. Digital Subscriber Line DSL and cable are two of the most common broadband connections. You can get a broadband connection by contacting an Internet service provider ISP. Typically, ISPs that provide DSL are telephone companies and ISPs that provide cable are cable TV companies. ISPs frequently offer broadband modems. Some ISPs also offer combination modem/wireless routers. Security is always important with a wireless network, it's even more important because your network's signal could be broadcast outside your home. If you don't help secure your network, people with PCs nearby could access info stored on your network PCs and use your Internet connection.

This helps protect your router. Most router manufacturers have a default user name and password on the router and a default network name also known as the SSID. Someone could use this info to access your router without you knowing it. To help avoid that, change the default user name and password for your router. See the documentation for your device for instructions. Wireless networks have a network security key to help protect them from unauthorized access. We recommend using Wi-Fi Protected Access 3 WPA3 security if your router and PC support it. See the documentation for your router for more detailed info, including what type of security is supported and how to set it up.

The wizard will walk you through creating a network name and a security key. If your router supports it, the wizard will default to WiFi Protected Access WPA2 or WPA3 security. We recommend that you use WPA3 if you can, because it offers better security than WPA2, WPA, or Wired Equivalent Privacy WEP security. With WPA3, WPA2 or WPA you can also use a passphrase, so you don't have to remember a cryptic sequence of letters and numbers. A firewall is hardware or software that can help protect your PC from unauthorized users or malicious software (malware). Running a firewall on each PC on your network can help control the spread of malicious software on your network, and help protect your PCs when you're accessing the Internet. Windows Firewall is included with this version of Windows.

There are many flavors of wireless being used for wireless broadband, Wimax, proprietary options, various satellite options, 2G/3G/4G/LTE and more. The many flavours cause a lot of marketing noise and "interference" for consumers trying to understand how their needs are met with each different flavour. On the positive side, wireless can be a great option for low-density and rural areas that don't have any wireline broadband options available. It can be fast to install with 24-hour turnarounds for a truck roll to install a small unit on the exterior of a business or home.

While Fiber To The Premise FTTP or FTTH is the ultimate solution for wireline delivery of braodband, the challenge is with the high build costs. In the vast majority of cities in North America – especially the rural and "near urban" cities and towns – there is no business case for a DSL/Cable operator to rip out their existing plants and rebuild using fiber from end to end. Only in specific cities, villages or countries that have had low wireline broadband implementation would it make sense to do a new build with high market penetration. There are many case studies that show a short term ROI for a large scale implementation, but so far most of the world is still lagging.

Importance

The need to have WPAN is increasing rapidly. As more and more individuals rely on electronic devices within their workspace or homes, a distinct need to have stable wireless connection among the devices has emerged. An ordinary individual is surrounded by computers, smartphones, smart TV, speakers, Wi-Fi powered devices, and whatnot. Connecting all these devices can be a challenge. Throw mobility in the mix and the challenge becomes impossible to handle. Because of its difficult nature, a need to have strong and stable WPAN technology becomes a necessity. A wireless network that is intended to cover an area that ranges around 31 miles or 50 kilometers is a WMAN. This specific branch of the network allows multiple locations or buildings to stay connected within any metropolitan area. It is used to connect different campuses of a single university, various blocks of a hospital, and multiple office buildings. The secure connection does not require a network of cables running from one building to the next. Instead, it relies on strong radio waves or infrared light to transmit data.

In a literal sense, Ad hoc means something improvised or a makeshift device. So, when it comes to defining it in terms of wireless technology, the wireless Ad Hoc network is a kind of impromptu, on-demand network that works from device to device. In this network setting, one can wirelessly connect one device to another without first connecting to a wireless router or Access Point. Since Ad Hoc wireless network can sustain itself without any existing infrastructure, it is decentralized and regarded as a peer-to-peer network. New devices in the market cannot cater to a wireless Ad hoc environment. However, there are still a few good reasons as to why one should invest in this networking technology. Since Ad hoc networks can be created in any environment and under any circumstances, this quality makes them ideal for larger organizations, SMEs, or ordinary personal usage.

Some wireless devices laptops, smart phones, or wireless routers support a mode called Ad-Hoc. This allows those devices to connect together directly, without an Access Point in-between controlling the connection. This forms a different type of network – in Ad-Hoc mode, all devices are responsible for sending and receiving messages to the other devices – without anything else in between. In an Ad-Hoc network, every device must be in this role, and using the same configuration to participate. Not all devices use this mode, and some have it as a "hidden" feature. An Ad-Hoc or Mesh node is similar to an individual in a group or roundtable discussion. They can take equal part in the conversation, raising their hand when they want to speak so the others will listen. If someone at the end of the table cannot hear, one of the individuals' in-between can repeat the original message for the listener.

A router acts as a home's unique connection to the internet: it consolidates your data traffic, protects your network, and sends the correct information to each device. For example, if one computer in home searches for a recipe on how to bake banana bread and a TV in the other room is streaming Netflix, you wouldn't want your banana bread recipe to show up on the TV and Netflix to pop up on the computer.