DESIGN OF LOW COST GENERIC WI-FI ACCESS POINT

...A low cost Wi-Fi solution

[1] **Kokkanti Tejaswini,** [2] **Prof. K Rama Naidu**
Electronics and Communication Engineering,
JNTUA, Ananthapuramu, India.

Abstract— We see that the deployment of Wireless Access Points is increasing rapidly from home-level to private enterprise Hotspots and to public hotspots. Wireless Access Point, WAP and Wireless LAN Controller, WLC are the key components of Wi-Fi Access Networks and CAPWAP (Control And Provisioning of Wireless Access Point) is a protocol used for communication among WAP and WLC. Prominently at enterprise level, generic components in Wi-Fi networks has become recent topic of interest. Generic components makes the existing network unbound and easily maintainable at reasonable costs and easily available and replaceable hardware components. This paper presents a detail on CAPWAP and related protocols, the way they are used. The current vendor interoperability issue is discussed along with different solutions under development. This paper also presents a generic access point built from scratch and working results of it as a stand-alone AP. Comparison with Controller based AP and possible future enhancements are also discussed.

Index Terms— CAPWAP, WI-Fi Protocol, Generic AP, Raspberry Pi, Channel, Frequency, Router, Switch, SSID; WAP/Wireless Access Point; WLC/Wireless LAN Controller.

I. INTRODUCTION

Wireless Networks allow mobility to its users for their convenience and to meet the growing needs for a reliable network on the go. Among different types of networks, (WAN, LAN, MAN, PAN), LAN has gained its importance in recent years especially the Wi-Fi. People rely more on Wi-Fi for an uninterrupted and a higher speed connectivity to internet. The growing interests in global connectivity and the advent of IoT has made Wi-Fi a basic amenity to this generation. With IoT, nearly every gadget will be internet connected or interconnected through internet. According to a survey conducted by OECD, it is predicted that by 2020, a household with two teenagers will have around 50 internet connected devices. These Wi-Fi compatible devices to be connected to Internet utilizes WLAN and Wireless Access Point with a backhaul and is based on IEEE 802.11 standard. A protocol is a set of rules that allow communication between two (minimum) entities. Here between Access Points and WLAN Controller. All these constitute key elements for a Wi-Fi Network Deployment.

WAP, Wireless Access Point is a networking hardware device, allows Wi-Fi compatible devices to be connected to the network. It bridges wireless traffic to the network. It may be standalone or Controller based access points. Controller or WLAN Controller along with some access point protocol, manages a group of access points by a network administrator at Network Operations Centre (NOC). WLC performs auto update of the firmware on the group of APs under its control when required. It directs and regulates traffic on a wireless network. There are different forms of Controller possible on Wireless networks. So also there is a possibility of having Controller-less solutions. Backhaul is the part of network which provides Signal (frequency) to the hotspot. The term backhaul may be used to describe the entire wired part of a network (although some part of networks have wireless instead of wired backhaul like as in mesh network) that may use a high-capacity wireless channel to get packets to the microwave or fiber links. The wireless network begins with a backhaul link from the core of the Internet service provider's network.

This thesis is organized as I. Introduction details about the topic of interest, Wi-Fi networks which is a part of Wireless Networks; II. Present State Of Art explains the current state of Wi-Fi, different existing issues currently troubling the Wi-Fi deployment and also various works going on with a motive towards addressing the existing issues and the objectives of present thesis; III. Actual Work is a detail on actual work flow and it explains why a Generic WAP can be a possible solution to the existing issues; IV. Result Discussion qualifies the work done in a project with the results obtained; V. Conclusion and Future Scope will conclude the thesis and suggests enhancements that can follow the actual work done.

II. PRESENT STATE OF ART

A. Current scenario

In case of home networking, it needs a single source and a standalone AP installed by the service provider and the higher functionalities managed by its ISP whereas lower functionalities can be customized at the customer end. It is simple. But when it comes to an enterprise hotspot or a city covering hotspots, it's not that simple. As we see we go to a public hotspot, switch on Wi-Fi on our devices, login to Wi-Fi, use the plan, recharge if needed. This is from the customer point of view. From the other end it is not as simple as that. We have stages of work is involved in Wi-Fi Deployment. The stages, Collection of customer requirements, Site design, Configuration and installation are more critical. Customer requirements will be carefully noted and documented with proper agreements. During site design, it is so important to check the possibilities to deploy the access points on the site after proper simulation. When the equipment is to be dumped, it is to be carefully noted the specifications and capabilities/quality of material. But it is not the only criteria. It is also important to check which particular vendor equipment is to be dumped. So this becomes a complex task. This is because as of now we have the access point communication protocols which works only between the products of single vendor from both the ends.

There are many makes of Access Points and Controllers available in the market. Most of the reliable quality products being proprietary and each of a different set of operability and command set. Loosely defined IEEE 802.11 standard is what makes this various flavors of Access Points and WLAN Controllers. IEEE 802.11 standard defined the functionalities to be implemented by combination of Access Point and

Controller. But the standard doesn't specify exactly how these functions are to be implemented or which of them to be implemented in which physical device.

Vendors take advantage of this flexibility in IEEE 802.11 architecture to come up with different configurations of WLAN services. The vendors also implement different value added services and functions such as Load balancing support, Quality of Service (QoS) and Rogue AP detection. The devices and firmware of one vendor is bound to be used among themselves only. Like, if a controller is of a particular make as of now it is that all the flow is locked to that vendor only in the sense that the WLAN controller, the WAP and the firmware are to be availed from the same vendor.

The following are the issues to be addressed in present field of art

- Vendor locked Wi-Fi components and firmware thereby missing Vendor-interoperability.
- The existing protocol allows communication between WAP and Controller of same Vendor and same type of components.
- Cost of reliable Wi-Fi solution is high and the market is in hands of some reputed vendors only.

B. Ongoing works on current issues

There are many works going on to address these issues in different possible ways.

One possible solution is to come up with an upgradation to the existing protocols like CAPWAP, LWAPP etc. to make them open sourced. This method needs the consent of the vendors which is not an easy task. Not all vendors agree with having a non-proprietary solution as this may reduce the prices of their manufactured product and get a high competitive market. At times this may lead some serious security issues if not given attention to.

The other possible solutions include building up some open-source platform like OpenRoads or openwincon to get a common platform for the existing networks. This solution is under development and the works are going on in different working groups like OpenFlow and OpenRoads under the supervision of Stanford University, COAP under University of Wisconsin Madison, openwincon sponsored by the Korean Government.

IEEE focuses on building up a middleware to get the interoperability into possibility. It supports NorthBound Interface and SouthBound Interfaces to be bound by a middleware which makes the open-source connectivity a reality. The working group, SDN-MCM - SDN based Middleware for Control and Management of Networks works for the project on middleware and 1930.1 - Recommended Practice for Software Defined Networking (SDN) based Middleware for Control and Management of Wireless Networks is the active project under IEEE is under progress.

C. Objectives

After observing all these issues and on-going works, our objectives will be

- to build a WAP using some easily available material in a cost effective manner.
- to configure this WAP as standalone WAP and check that it is in working condition.
- to connect it through a router or a switch and compare it's working.

III. ACTUAL WORK

There is a possibility of building a Generic Access Point and/or a Generic Wireless LAN Controller and getting them connected through the existing protocols as a solution for the fore-discussed objectives. We consider building a Generic Access Point. The reason behind choosing to develop a Generic WAP but not a Generic WLAN Controller is that the Controller is the device at NOC end or at the ISP end. So we focus on the device at the customer end and which can be customized with our possibilities, the Wireless Access Point. By this we address the interoperability issue to some extent now and completely with some future work possible (connecting the complete set to the WLAN controller). We are also addressing 3rd listed issue to build a cost effective Wi-Fi solution.

A. Generic Wi-Fi Access Point

A Generic AP is a device with all the generic features. Here the proprietary nature of the component is either supressed or open-sourced. By doing so, though the communication protocol is not open-sourced, there is a possibility of getting it connected to different controllers.

B. Base of Work

In general there will be a router or switch between an Access point and a controller. So our Access Point needs to be connected to the Switch or the Router first. Then we can try the set to be connected to a controller. This makes the most complex work a little simple.

With this idea, we step towards a possible solution to the existing problem by building a Generic Access Point.

In order to build an Access Point, Radio transceiver, Antenna and Ethernet port are key requirements. It is needed that it should consume low power thereby dissipating less amount of heat.

In general a single radio can serve up to 25 clients and it is required to support the set of frequencies we are supposed to use for our Wi-Fi service. Antenna decides the coverage range of access point. Ethernet port is needed to connect the access point to the wired backhaul such as cat-5 or cat-6 Ethernet cable.

Choosing Raspberry Pi model 3 is a good option as it has more specifications matching our requirement.

C. Choosing Raspberry Pi

Raspberry Pi can be said as a low power Linux based mini Processor hardly the size of our palm, mainly used for research purpose. The Raspberry Pi we chose is Raspberry Pi 3, Model B.

It has an inbuilt Wi-Fi capable Radio, BCM43438 Wi-Fi adapter chip located just beside the Micro SD card port on the rear side of RPi3. It supports 2.4GHz 802.11n Wireless LAN with 10/100 Ethernet Port and a Bluetooth Radio support. It works with a DC input of 5V and 2.4A which can be powered by a micro USB power input.

In the Front view of RPi3, we can see a black chip labelled Broadcom BCM2837 which is a Quad core 64 bit processor and it runs at 1.2GHz and has 1GB of RAM inbuilt with a processing speed of 900MHz. It has an extendable 40 pin GPIO and four externally usable 2.0 USB ports.

It also accommodates some other features like CSI, DSI, full size HDMI interface (3.5mm 4-pole Composite Audio-Video output Jack).

Two Serial Interface ports can be seen on the front view of Raspberry Pi 3 the one besides the HDMI port is the Camera serial Interfacing port (CSI) and the other seen to the edge vertically between micro USB power port and the on-board antenna is Display Serial Interface, DSI port.

D. Work flow

Raspberry Pi 3 board is connected with a Monitor (via HDMI), Keyboard and Mouse (via USB). For internet connection, connect with one Ethernet cable or to some Wi-Fi available. We have connected an Ethernet cable for Internet Connection. Before giving power supply, we need to mount the SD card and check for proper connections.

Since it is small device, there is a high chance of processor getting over heated which may in turn lead to device breakdown as we give it a prolonged load in this case.

So we use Heat sinks on the processor. The Heat sinks are made of Aluminum (mostly but copper heat sinks are also available in the market) with a thermal adhesive at the back to make the installation hassle free.

Preparing SDcard:

Micro SDcard above 8GB is reliable. So, we took a 16GB Micro SDcard.

Open Terminal Window where one can program on Command Line Interface (CLI). CLI is more secured than GUI and is better supported as we are using Linux based OS on it. Check the Internet connection to the RPi (We can Ping some website or the DNS Server via Terminal to know). The DNS ids 8.8.8.8 and 8.8.4.4 are Google Public DNS server IP for IPv4service.

Check on the RPi screen to find the available interfaces. On RPi3, if we could see both Ethernet and WLAN interfaces, connect to available internet source (We connected an Ethernet cable for internet source). With active Internet connection, update all the packages to the latest version.

Now enable WLAN interface (Check it by scanning for the available SSIDs).

Each SSID radiating will be treated as a Cell. Cell is a basic coverage zone. Each cell will have some attributes the assigned channel, its Frequency, Quality, Signal level, Encryption, Bitrates and mode of access point.

Check with the NIC card for "Supported interface modes". If AP mode is available, configuration will be proceeded, else we have to go for an add-on NIC and configure it for our device before proceeding. Here we use BCM 43438 as Network card.

With active Internet connection, install the basic dependencies (packages) required (with changes in configuration files as per our requirement). We need DNS forwarding and Dynamic Host Configuration Protocol server as the basic firmware requirements for building an Access Point. The daemons, DNSMASQ and UDHCPD are supporting files for the DNS forwarding and user DHCP server for smaller networks. Re-configure these daemons to make them compatible with our hardware. Make Authoritative the DHCP server for the local network. It enables the DHCP service to provide client IPs. After enabling DHCP server, provide IP ranges, lease times, subnet mask and network gateway details in a file and save them conveniently to be used when enabling Access point. Include WLAN in the interfaces and set up a DHCP server on the device. In this setup we configure the server so that it could be able to assign IP to its clients. The lease time and idle time are to be configured.

Now that DHCP server is set up to distribute IP addresses to the clients, our device needs NAT tables. We go with IPv4 and so we build IP-tables use policy. To build IP-tables policies, first the system control is to be given for ip-forwarding (i.e., allow IP-forwarding by the system controls). The interfaces need to understand the IP-table policies for better client support. So, the path is given for the interfaces towards iptables.ipv4.nat where IP-Table policies are devised. Here care is needed to check the IP range provided by DHCP server set up matches the IPv4 IP-table policies we built.

Build WLAN in interfaces and make the WLAN as the default interface. Since it is easy for a default interface to support DHCP server initial scripts. Since Access point needs an IP to radiate, provide an IP to (radiating) WLAN interface. By this configuration, we make the WLAN port capable of radiating instead of scanning for SSIDs to get connected to.

Once this configuration is done, set the basic and advanced configurations (which ever are mandatory as per our need) needed for the Access Point. For this make a configuration file (with .conf extension) and give all parameter values in that file and save the file at accessible location so that we can easily access it or set path to it for background programs we build to run it when required.

The configuration file must include basic set of configurations like interface used, band utilized and encryption type. These basic configurations are mandatory and there are certain features which allow us to enhance the cell configuration. These include channel assignment, Country code, frequency limits can be provided but not mandatory as they will be assigned with the defaults when not mentioned. Other features like QoS support, DFS, Capabilities, preamble are advanced features and can be used if necessary.

Here are some of the inputs given in the configuration file (Wi-Fi related configurations). We chose 2.4 GHz Wi-Fi band and for that, IEEE802.11b standard is chosen. WLAN interface is associated to AP. Some free channel is selected which has less interference factor (Interference to certain channel at a given area can be checked by using iBWave tool). Mode of encryption selected and provided authentication using passcode.

An Access Point also needs a provision to Authorize, Authenticate and Account listing of its users or clients. RADIUS server can serve AAA services. So, RADIUS server is built for our device.

Include each of these service configuration paths in the user service bin in proper sequence. The user service bin allows the binaries to start or stop or run in background according to their configurations written there in. Once we find that everything is in order and fine, we direct the service bin to the Wi-Fi related configuration file we have saved with detail of SSID and encryption methods.

With this, AP starts radiating with the SSID we have provided.

IV. RESULT DISCUSSION

To qualify as an Access Point, the basic requirement is to be able to radiate with the provided SSID. SSID provided by the user during the WAP configuration and the SSID displayed on the display screen of gadget (Mobile) connected to the WAP through SSID must be the same. Fig. 1 shows the CLI screen of the built AP and Fig. 2 shows the display screen of gadget connected to this SSID (Wi-Fi connected Gadget). In that we see that the AP is enabled and ssid provided is the one radiating and it is "Trail_AP". We can identify from the CLI output that WLAN interface set up (WLAN0) is used to radiate, accounting sessions are served by the radius server we have setup for the device, each client is connected via its MAC ID and a unique IP is assigned to each client or end user.

```
Using interface wlan0 with hwaddr b8:27:eb:e5:63:0d and ssid "Trial_AP"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED
wlan0: STA 9c:a5:c0:f6:59:57 IEEE 802.11: associated
wlan0: AP-STA-CONNECTED 9c:a5:c0:f6:59:57
wlan0: STA 9c:a5:c0:f6:59:57 RADIUS: starting accounting session 58F4A53F-00000000
wlan0: STA 9c:a5:c0:f6:59:57 WPA: pairwise key handshake completed (RSN)
wlan0: STA 2c:33:61:5e:3f:62 IEEE 802.11: associated
wlan0: AP-STA-CONNECTED 2c:33:61:5e:3f:62
wlan0: STA 2c:33:61:5e:3f:62 RADIUS: starting accounting session 58F4A53F-00000001
wlan0: STA 2c:33:61:5e:3f:62 WPA: pairwise key handshake completed (RSN)
wlan0: STA 9c:a5:c0:f6:59:57 WPA: group key handshake completed (RSN)
wlan0: STA 2c:33:61:5e:3f:62 WPA: group key handshake completed (RSN)
wlan0: STA 2c:33:61:5e:3f:62 WPA: group key handshake completed (RSN)
wlan0: AP-STA-DISCONNECTED 9c:a5:c0:f6:59:57
WPA: wpa_sm_step() called recursively
wlan0: STA 9c:a5:c0:f6:59:57 IEEE 802.11: disassociated
wlan0: STA 9c:a5:c0:f6:59:57 IEEE 802.11: associated
wlan0: AP-STA-CONNECTED 9c:a5:c0:f6:59:57
wlan0: STA 9c:a5:c0:f6:59:57 RADIUS: starting accounting session 58F4A53F-00000002
wlan0: STA 9c:a5:c0:f6:59:57 WPA: pairwise key handshake completed (RSN)
 wlan0: STA 2c:33:61:5e:3f:62 WPA: group key handshake completed (RSN)
wlan0: AP-STA-DISCONNECTED 9c:a5:c0:f6:59:57
WPA: wpa_sm_step() called recursively
wlan0: STA 9c:a5:c0:f6:59:57 IEEE 802.11: disassociated
wlan0: STA 9c:a5:c0:f6:59:57 IEEE 802.11: associated
wlan0: AP-STA-CONNECTED 9c:a5:c0:f6:59:57
wlan0: STA 9c:a5:c0:f6:59:57 RADIUS: starting accounting session 58F4A53F-00000003
wlan0: STA 9c:a5:c0:f6:59:57 WPA: pairwise key handshake completed (RSN)
```

Fig. 1: CLI output showing Access Point radiating and clients connected

It shows that MAC IDs 9c:a5:c0:f6:59:57 and 2c:33:61:5e:3f:62 are authenticated and for the same, AP-STA connection is established. Here AP is Wireless Access Point and STA is Station or end-user or client. lease time is set to 10 minutes So, when a station is idle (not accessing internet) for a span of 10 minutes, it is disconnected and then pinged again to see if it is still in range. After 10minutes of inactivity (idle time), device with MAC ID 9c:a5:c0:f6:59:57 is still in range and so reconnected and its IP will be retained. Device with MAC ID 2c:33:61:5e:3f:62 is not in range and so is not reconnected and its IP will be disassociated. Here the statistics can be collected session wise.

As we have discussed, unique IP should be assigned to each client. When an IP is assigned to a client on authenticating one's MAC ID, the end user should get proper access to internet. DNS server is basic requirement for the internet access and 8.8.8.8 is the Google's public DNS.

Fig. 3 endorse the basic DNS server is accessible from its ping statistics. To recheck further we confirm the connectivity to some website. In Fig , the second ping statistics shows that we have checked with the connectivity with the most used search engine site, Goolge.com and it is displayed that there is no/zero loss. We see 216.58.197.78 is the IP pinged when we commanded to ping google.com which says that google.com IP is 216.58.197.78 which is true. There is no packet loss, so the packet transmission is perfect and the device is accessing a good internet connection.

The Access Point built out of scratch and its authentication is through RADIUS and Encryption through WPA2 (using Passcode which is latest and reliable). Number of SSIDs (maximum 8) could be set to group different classes of end users.

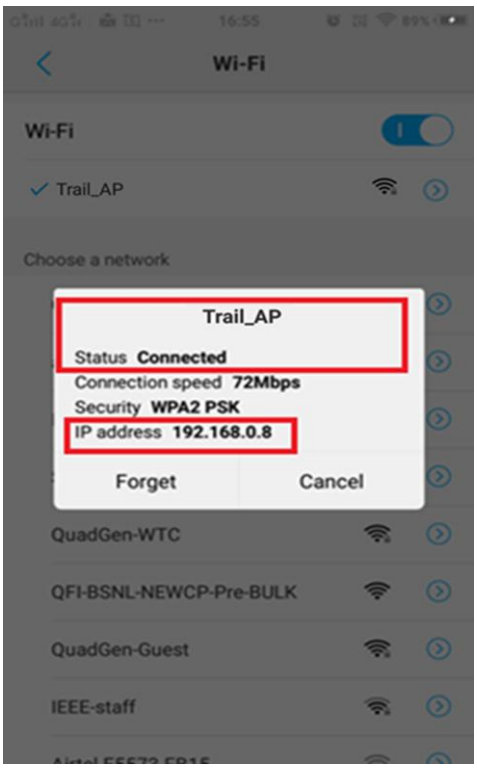

Fig. 2: SSID radiating and IP assignment to connected clients

With the results that are discussed (with valid screenshots) predicate that the access point is working as per requirement as a standalone Wireless Access Point.

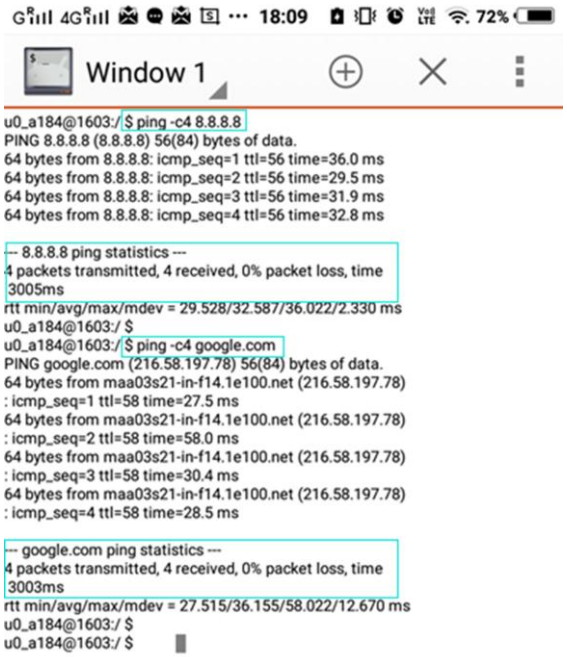

Fig. 3: Checking the Internet access in connected device/gadget

Also the cost of WAP is also reduced. The cost of one of the leading and reliable WAP, Cisco K9 Aironet WAP is around □ 70,000. The Generic AP we built costs at the most □ 4000 (raspberry Pi= □ 2500; add-on NIC chip= □ 300; Radio chip= □ 500) and a bit of programming is needed to get a capacity of 200 users.

A. Summarized Results

All the discussed results are summarized in the following table.

Table 1: Results Summarized

Result	Reference	Remarks
SSID radiating with correct name provided	Fig 1	✓
Number of clients connected (authenticated via MAC ID)	Fig 1	✓
AAA service by RADIUS server	Fig 1	✓
WPA2 Encryption (WPA2 PSK)	Fig 1	✓
IP assignment to clients connected	Fig 2	✓
Clients connected having proper internet access	Fig 2 and Fig 3	✓
No Packet loss (Good coverage and capacity)	Fig 3	✓

V. Conclusion and Future Enhancements:

In this paper we present details on present field of art, Wi-Fi, a part of Wireless communications, the current scenario of Wi-Fi Networks, existing issues are discussed. Some ongoing projects to address the issues are detailed and the Generic Wi-Fi Access Point is defined and built to be a standalone WAP using low cost material and its working is discussed with results.

The possible future enhancement of this project is making the built Generic WAP work as a controller-based WAP.

References

[1] https://tools.ietf.org/html/rfc5415
[2] https://learningnetwork.cisco.com/thread/62908
[3] https://supportforums.cisco.com/t5/wireless-mobility-documents/capwap-encryption-using-dtls/ta-p/3148917
[4] http://lets-start-to-learn.blogspot.in/2014/08/cisco-wireless-understand-capwaplwapp.html
[5] https://en.wikipedia.org/wiki/CAPWAP
[6] https://www.raspberrypi.org/forums/

[7] https://www.raspberrypi.org/documentation/installation/noobs.md
[8] https://learn.adafruit.com/setting-up-a-raspberry-pi-with-noobs/download-noobs
[9] http://lets-start-to-learn.blogspot.in/2014/08/cisco-wireless-understand-capwaplwapp.html
[10] http://what-when-how.com/deploying-and-troubleshooting-cisco-wireless-lan-controllers/overview-of-capwap-cisco-wireless-lan-controllers/
[11] https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/69561-wlc-faq.html
[12] https://supportforums.cisco.com/t5/getting-started-with-wireless/how-does-capwap-work-when-an-lwap-and-wlc-are-not-on-the-same/td-p/2448765
[13] https://www.cisco.com/c/en/us/support/docs/wireless/wireless-lan-controller-software/118833-wlc-design-ftrs-faq.html
[14] http://www.iac.rm.cnr.it/~massimo/Papers/COMNET.pdf
[15] http://onlinelibrary.wiley.com/doi/10.1002/nem.1949/abstract
[16] http://www.cse.wustl.edu/~jain/cse574-10/ftp/capwap/index.html
[17] http://ieeexplore.ieee.org/document/4488132/
[18] https://wiki.openwrt.org/about/start
[19] https://wiki.openwrt.org/toh/start
[20] http://www.makeuseof.com/tag/what-is-openwrt-and-why-should-i-use-it-for-my-router/
[21] https://lede-project.org/
[22] www.netconfcentral.org/netconf_docs
[23] https://www.networkworld.com/article/.../tech.../understanding-netconf-and-yang.html
[24] https://tools.ietf.org/html/rfc6241
[25] https://documentation.meraki.com/zGeneral_Administration/Tools_and_Troubleshooting/Fundamentals_of_802.1Q_VLAN_Tagging
[26] https://www.domotz.com/wi-fi-facts/
[27] http://www.internetworldstats.com/stats.htm
[28] https://www.domotz.com/wi-fi-facts/
[29] https://en.wikipedia.org/wiki/List_of_countries_by_number_of_Internet_users
[30] http://www.internetworldstats.com/stats.htm
[31] https://en.wikipedia.org/wiki/IEEE_802.11
[32] CWDP Certified Wireless Design Professional Official Study Guide: Exam PW0-250 by Shawn M. Jackman, Matt Swartz, Marcus Burton, Thomas W. Head
[33] Wi-Fi Enabled Healthcare by Ali Youssef, Douglas McDonald II, Jon Linton, Bob Zemke, Aaron Earle
[34] http://www.annese.com/blog/wireless-lan-controllers
[35] https://www.cisco.com/web/AP/wireless/pdf/Benefits_of_centralizedWLan.pdf
[36] https://www.securedgenetworks.com/blog/controller-vs-controllerless-wifi-whats-the-difference
[37] http://www.annese.com/blog/wireless-lan-controllers
[38] http://www.embedur.com/CS023_270313.pdf
[39] https://www.raspberrypi.org/downloads/noobs/
[40] https://standards.ieee.org/develop/wg/SDN-MCM.html
[41] https://standards.ieee.org/develop/project/1930.1.html