RAMAIAH UNIVERSITY OF APPLIED SCIENCES

# ASSIGNMENT

| | |
|---|---|
| Course Code | 19CSC303A |
| Course Name | Computer Networks |
| Programme | B. Tech |
| Department | Computer Science and Engineering |
| Faculty | Engineering and Technology |

| | |
|---|---|
| Name of the Student | Deepak R |
| Reg. No | 18ETCS002041 |
| Semester/Year | 5th/2020 |
| Course Leader/s | Dr. Rinki Sharma |

## Declaration Sheet

| | | | |
|---|---|---|---|
| Student Name | Deepak R | | |
| Reg. No | 18ETCS002041 | | |
| Programme | B. Tech | Semester/Year | 5th/2020 |
| Course Code | 19CSC303A | | |
| Course Title | Computer Networks | | |
| Course Date | | to | |
| Course Leader | Dr. Rinki Sharma | | |

**Declaration**

The assignment submitted herewith is a result of my own investigations and that I have conformed to the guidelines against plagiarism as laid out in the Student Handbook. All sections of the text and results, which have been obtained from other sources, are fully referenced. I understand that cheating and plagiarism constitute a breach of University regulations and will be dealt with accordingly.

| | | | |
|---|---|---|---|
| Signature of the Student | | Date | |
| Submission date stamp<br>(by Examination & Assessment Section) | | | |

| Signature of the Course Leader and date | Signature of the Reviewer and date |
|---|---|
| | |

| Faculty of Engineering & Technology | | | |
|---|---|---|---|
| Ramaiah University of Applied Sciences | | | |
| Department | Computer Science and Engineering | Programme | B. Tech. |
| Semester | 5th | | |
| Course Code | CSC303A | Course Title | Computer Networks |
| Course Leader | Dr. Rinki Sharma, Ms. Suvidha K S, Mr. Nithin Rao R | | |

| Assignment - 2 | | | |
|---|---|---|---|
| Register No. | 18ETCS002041 | Name of Student | Deepak R |

| Sections | | Marking Scheme | Max Marks | First Examiner Marks | Second Examiner Marks |
|---|---|---|---|---|---|
| Q1 | 1.1 | Introduction to VLSM | 01 | | |
| | 1.2 | Difference between VLSM and CIDR | 02 | | |
| | 1.3 | Advantages of using VLSM and CIDR together in a single network | 02 | | |
| | | Max Marks | 05 | | |
| Q2 | 2.1 | Differentiate among IEEE 802.11 Wi-Fi protocols 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax w.r.t data rate, bandwidth, frequency band and access techniques | 10 | | |
| | 2.2 | Explain the different encryption techniques used in IEEE 802.11 Wi-Fi protocols. | 10 | | |
| | | Max Marks | 20 | | |
| | | Total Assignment Marks | 25 | | |

| Course Marks Tabulation | | | | |
|---|---|---|---|---|
| Component- 1(B) Assignment | First Examiner | Remarks | Second Examiner | Remarks |
| Q 1 | | | | |
| Q 2 | | | | |
| Marks (Max 25 ) | | | | |
| Signature of First Examiner | | | | Signature of Second Examiner |

Please note:

1. Documental evidence for all the components/parts of the assessment such as the reports, photographs, laboratory exam / tool tests are required to be attached to the assignment report in a proper order.
2. The First Examiner is required to mark the comments in RED ink and the Second Examiner's comments should be in GREEN ink.
3. If the variation between the marks awarded by the first examiner and the second examiner lies within +/- 3 marks, then the marks allotted by the first examiner is considered to be final. If the variation is more than +/- 3 marks then both the examiners should resolve the issue in consultation with the Chairman BoE.

## Assignment

Instructions to students:

1. The assignment consists of 3 questions.
2. Maximum marks is 25.
3. The assignment has to be neatly word processed as per the prescribed format.
4. The maximum number of pages should be restricted to 9.
5. The printed assignment must be submitted to the course leader.
6. Submission Date: January 22nd 2021
7. Submission after the due date is not permitted.
8. IMPORTANT: It is essential that all the sources used in preparation of the assignment must be suitably referenced in the text.
9. Marks will be awarded only to the sections and subsections clearly indicated as per the problem statement/exercise/question

## Solution to Question 1

## Introduction to VLSM.

A Variable Length Subnet Mask (VLSM) is a numerical masking sequence, or IP address subset, based on overall network requirements. A VLSM allows a network administrator to use long masks for networks with few hosts and short masks for networks with multiple hosts. A VLSM is used with a VLSM router and must have routing protocol support.

A VLSM is also known as a classless Internet Protocol (IP) address.

VLSM is similar in concept and intent to Classless Inter Domain Routing (CIDR), which allows a single Internet domain to have an address space that does not fit into traditional address classes. VLSM was originally defined in IETF RFC 1812.

## Difference between VLSM and CIDR

CIDR is the chunk of meat the provider gives you, VLSM is how you serve it to your guests

- CIDR is a concept applied more at the ISP/Provider level. VLSM is a concept applied more at interior routing within an enterprise; a mechanism used by the recipient of a CIDR block.
- CIDR allows super-netting for efficient advertisement and summarization of the domains at the higher level. For example, if an ISP owns network 172.16.0.0/16, then the ISP can offer 172.16.1.0/24, 172.16.2.0/24, and so on to customers. Yet, when advertising to other providers, the ISP only needs to advertise 172.16.0.0/16; This helps in reducing the size of full Internet BGP table
- If the ISP / provider gives you a /24 CIDR block, you will likely use VLSM to subnet it into a smaller blocks

CIDR helps us to clearly delineate the addresses that use by setting up a prefix notation instead of using a subnet mask to make it easier to use VLSM.

So one is a method (VLSM) of doing, the other is a method of reporting what is done.

## Advantages of using VLSM and CIDR together in a single network

**By Using CIDR and VLSM together in a Single network we can reduce the number of routing table entries ,Greater efficiency, any number of contiguous bits can be assigned to identify networks, depending on the number of hosts it needs to support. This will greatly reduce the number of wasted IP addresses. For example, let us say a network has 900 hosts. If classful IP addressing is used, this network needs 4 class C IP addresses or one class B IP address. If a class B IP address is used, as the maximum number of hosts in a class B network is 65534, a very large number (65534 - 900) of host IP addresses will be wasted. As the number of class C IP networks is limited (2097152), it is not preferable to assign 4 class C IP addresses to this network. On the other hand, if CIDR is used, then this network can be assigned an IP address with a network prefix of 22 (i.e. /22). This means, 10 bits are available for hosts, resulting in 1024 available host IP addresses, satisfying the exact requirements of the network. So by combining VLSM and CIDR the IP address space can be effectively used, Multiple networks can be shared with a single 'summary' address which reduces routing table size and makes route lookups faster.So it is advisible to combine both VLSM and CIDR together in a single network.**

**Solution for Question 2**

## Solution for 2.1

The IEEE802.11 standard was released by the IEEE (LAN/MAN) standard committee on June 1997. Since then multiple upgrades have been released to catch up with advancements in the communication technologies

**A. IEEE802.11a**

The IEEE802.11a standard was released on September 1999. Networks using 802.11a operate at radio frequency of 5GHz or 3.7GHz and a bandwidth of 20MHz. The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that is especially well suited to use in office settings. In 802.11a, data speeds as high as 54 Mbps are possible. This standard employ the single input, single output (SISO) antenna technologies, and the indoor/outdoor ranges from 35m to 125m for 5GHz operating frequency. The outdoor range goes to 5Km for operating frequency of 3.7G. The IEEE802.11a is less prone to interference compared to with 802.11b due to the high operating frequency of 5GHz.

**B. IEEE 802.11b**

IEEE 802.11b standard was released on September 1999 as well. This standard provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz operating frequency and bandwidth of 22MHz. The 802.11b uses only DSSS (Direct Sequence Spread Spectrum) modulation technique. This standard also employs the SISO antenna technology as in the IEEE802.11a standard. The IEEE802.11b standard was ratified on 1999 from the original IEEE802.11 standard which allowed wireless functionality comparable to Ethernet. The IEEE802.11b standard is prone to higher interference due to the fact that the 2.4GHz frequency range is becoming crowded with carriers, hence increased interference risk. The indoor and outdoor ranges for this standard is 35m to 140m.

**C. IEEE 802.11g**

The standard 802.11g was ratified in 2003 as an IEEE standard for Wi-Fi wireless networking and it supports maximum network bandwidth of 54 Mbps compared to 11 Mbps for 802.11b. This standard operates at 2.4GHz frequency and bandwidth of 20MHz. This standard uses the OFDM or DSSS modulation schemes. This standard employ the SISO antenna technologies, and its indoor/outdoor range are from 38m to 140m respectively.

**D. IEEE 802.11n**

The 802.11n standard was ratified in 2009 and it utilizes multiple wireless antennas in tandem to transmit and receive data[3-4]. The IEEE802.11n standard employs OFDM modulation technique. The antenna technology used with the IEEE802.11n standard is known as Multiple Input, Multiple Output (MIMO). This technology refers to the ability of 802.11n and similar technologies to coordinate multiple simultaneous radio signals. The MIMO increases both the range and throughput of a wireless network. An additional technique employed by 802.11n involves increasing the channel bandwidth from 20MHz to 40MHz. The 802.11n standard support maximum theoretical network bandwidth up to 300 Mbps. The IEEE802.11n indoor/outdoor ranges are 75m, and 250m respectively.

### E. IEEE 802.11ac

IEEE 802.11ac is the fifth generation in Wi-Fi networking standards released December 2013[5-6]. This standard operating frequency is 5GHz, and bandwidth of 20, 40, 80, 160MHz sectors. The stream rates ranges for these bandwidth sectors are 7.2 - 96.3Mbps for 20MHz, and 15 – 200Mbps for 40MHz, 32.5 - 433.3Mbps for 80MHz, and 65 - 866.7Mbps for 160MHz. This standard exhibits better performance, and better coverage compared to IEEE 802.11a,b,g and n standards. The 802.11ac standard uses a wider channel and an improved modulation scheme that also supports more clients. The IEEE 802.11ac standard utilizes a modulation technique known as multi-user MIMO. This technique allows a set of users or wireless terminals, each with one or more antennas, o communicate with each other. The indoor range is 35m, and there is no recorded max for outdoor range.

### F.IEEE 802.11ax

Is the successor to 802.11ac, and will increase the efficiency of WLAN networks. This project has the goal of providing 4x the throughput of 802.11ac at the user layer, having just 37% higher nominal data rates at the PHY layer. The 802.11ax standard is expected to become an official IEEE specification in September 2020. In the previous amendment of 802.11 (namely 802.11ac), Multi-User MIMO has been introduced, which is a spatial multiplexing technique. MU-MIMO allows the Access Point to form beams towards each Client, while transmitting information simultaneously. By doing so, the interference between Clients is reduced, and the overall throughput is increased, since multiple Clients can receive data at the same time. With 802.11ax, a similar multiplexing is introduced in the frequency domain, namely OFDMA. With this technique, multiple Clients are assigned with different Resource Units in the available spectrum. By doing so, an 80 MHz channel can be split into multiple Resource Units, so that multiple Clients receive different type of data over the same spectrum, simultaneously. In order to have enough subcarriers to support the requirements of OFDMA, four times as many subcarriers are needed than by the 802.11ac standard. In other words, for 20, 40, 80 and 160 MHz channels, there are 64, 128, 256 and 512 subcarriers in the 802.11ac standard, but 256, 512, 1024 and 2048 subcarriers in the 802.11ax standard. Since the available bandwidths have not changed and the number of subcarriers increases by a factor of 4, the subcarrier spacing is reduced by the same factor, which introduces 4 times longer OFDM symbols: for 802.11ac the duration of an OFDM symbol is 3.2 microseconds, and for 802.11ax it is 12.8 microseconds (both without guard intervals).

**Continued->**

## Further Comparison Between IEEE 802.11a,b,g,n and ac and ax additional features

| Feature | 802.11a | 802.11b | 802.11g | 802.11n | 802.11ac | 802.11ax |
|---|---|---|---|---|---|---|
| Beamforming | No | No | No | Yes | Yes | Yes |
| Coverage | Low | Low | Low | Low | High | High |
| Capacity | Low | Low | Low | Low | High | High |
| Interference | More on 2.4GHz<br>Less on 5GHz | More | More | More on 2.4GHz<br>Less on 5GHz | Less | Less |
| Quality | Low | Low | Low | Low | High | High |

## Solution for 2.2

Encryption is the process of converting data into a cryptic format or code when it is transmitted on a network. Encryption prevents unauthorized use of the data.

nstant supports the following types of encryption:

- WEP —Wired Equivalent Privacy (WEP) is an authentication method where all users share the same key. WEP is not secure as other encryption types such as TKIP.
- TKIP —Temporal Key Integrity Protocol (TKIP) uses the same encryption algorithm as WEP . However, TKIP is more secure and has an additional message integrity check (MIC).
- AES — The Advanced Encryption Standard (AES) encryption algorithm a widely supported encryption type for all wireless networks that contain any confidential data. AES in Wi-Fi leverages 802.1X or PSKs to generate per station keys for all devices. AES provides a high level of security like IP Security (IPsec) clients.

WEP and TKIP are limited to WLAN connection speed of 54 Mbps. The 802.11n connection supports only AES encryption. Aruba recommends AES encryption. Ensure that all devices that do not support AES are upgraded or replaced with the devices that support AES encryption.

### WPA and WPA2

WPA is created based on a draft of 802.11i, which allowed users to create more secure WLANs. WPA2 encompasses the full implementation of the 802.11i standard. WPA2 is a superset that encompasses the full WPA feature set.

The following table summarizes the differences between the two certifications:

Table 1: *WPA and WPA2 Features*

| Certification | Authentication | Encryption |
|---|---|---|
| WPA | l PSK<br>lIEEE 802.1X with Extensible Authentication Protocol (EAP) | TKIP with message integrity check (MIC) |
| WPA2 | l PSK<br>lIEEE 802.1X with EAP | AES -- Counter Mode with Cipher Block Chaining Message Authentication Code (AESCCMP) |

**WPA and WPA2 can be further classified as follows:**

- **Personal —** Personal is also called Pre-Shared Key (PSK).
  In this type, a unique key is shared with each client in the network.
  Users have to use this key to securely log in to the network.
  The key remains the same until it is changed by authorized personnel.
  we can also configure key change intervals .
- **Enterprise —** Enterprise is more secure than WPA Personal.
  In this type, every client automatically receives a unique encryption key after securely logging on to the network. This key is automatically updated at regular intervals. WPA uses TKIP and WPA2 uses the AES algorithm.

**Recommended Authentication and Encryption Combinations**

The following table summarizes the recommendations for authentication and encryption combinations for the Wi-Fi networks.

Table 2: *Recommended Authentication and Encryption Combinations*

| Network Type | Authentication | Encryption |
|---|---|---|
| Employee | 802.1X | AES |
| Guest Network | Captive Portal | None |
| Voice Network or Handheld devices | 802.1X or PSK as supported by the device | AES if possible, TKIP or WEP if necessary (combine with security settings assigned for a user role). |

## References

*Computer Networks* 5th Edition is a *book* authored by Andrew S. Tanenbaum and David J. Wetherall.