RAMAIAH UNIVERSITY OF APPLIED SCIENCES

ASSIGNMENT 2

Course Code	CSC303A
Course Name	Computer Networks
Programme	B. Tech.
Department	Computer Science and Engineering
Faculty	FET

Name of the Student	Subhendu Maji
Reg. No	18ETCS002121
Semester/Year	5TH SEM / 2018 BATCH
Course Leader/s	Mr. Nithin Rao R

Declaration Sheet				
Student Name	Subhendu Maji			
Reg. No	18ETCS002121			
Programme	B. Tech.		Semester/Year	5th sem / 2018 batch
Course Code	CSC303A			
Course Title	Computer Networks			
Course Date		to		
Course Leader	Mr. Nithin Rao R			

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 (by Examination & Assessment Section)			

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

Contents

Assignment - 2					
Register No.	**18ETCS002121**	Name of Student	**SUBHENDU MAJI**		

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

Question No. 1

Solution to Question No. 1:

1.1 Introduction to VLSM

VLSM (Variable Length Subnet Masking) is a technique of assigning the host space of distinct size between the networks through distributing a network into several subnetworks. It was basically designed to provide more flexibility for configuring a network using different masks.

In other words, the Variable Length Subnet Masking or VLSM is the technique of applying multiple subnet mask to a provided class of addresses over a routed system. This was not possible before as the previously designed protocols like RIPv1 would not support subnet mask of advertised networks in their routing updates. As an outcome, they are unable to learn the existence of more than one mask length.

The classless routing protocols like OSPF, RIPv2, EIGRP, IS-IS and BGP make the implementation of VLSM possible by incorporating the subnet mask for the networks that are advertised in the routing updates. Previously, the use of networks was limited to only/26 masks throughout the system.

Example:
Let's take an example of a university which has several departments with different computing needs, such as engineering department needs 75 hosts, management department needs 50, similarly arts department with 25 and medical science department with 20. Here, we are taking regular class C address space – 192.168.1.0. If we employ fixed subnetting in the above example, the 255 host addresses will be divided into 4 subnets of 62 hosts. Therefore, the engineering department will experience a shortage of IP addresses while medical science department would get IP addresses in abundance.

So, resolve this issue VLSM (Variable Length Subnet Masking) is used, the 255 addresses are first divided into two parts each having 126 hosts. One subnet will be allotted to the engineering department. The other subnet is divided into two sub-subnets each having 62 hosts, among which one is assigned to the management department. Similarly, the sub-subnet with 62 hosts is further split to generate two sub-sub-subnets containing 30-30 hosts each which covers the remaining two departments.

1.2 Difference between VLSM and CIDR

CIDR (Classless Interdomain Routing)	VLSM (Variable Length Subnet Masking)
CIDR is the summarization of the subnets back to the classes.	VLSM permits us to apply variable subnet masks to the same class address space.
In simple words, it enables routers to group routes together.	In simple words, it facilitates in optimizing the available address space.
CIDR uses super-netting which refers to the aggregation of the network in a single address.	VLSM employs the concept of the subnetting which is nothing but the subdivision of one network into multiple sub-addresses.
The protocols that assist CIDR are BGP and OSPF.	The protocols that assist VLSM are RIPv2, OSPF, IGRP, and BGP.
Merits: • Reduces the size of the routing table. • Generates less overhead with respect to network traffic, CPU and memory. • Provides flexibility in designing, addressing the networks.	Merits: • Effective utilization of the address space. • It is capable of hierarchical addressing. • Reduces the size of the routing tables.

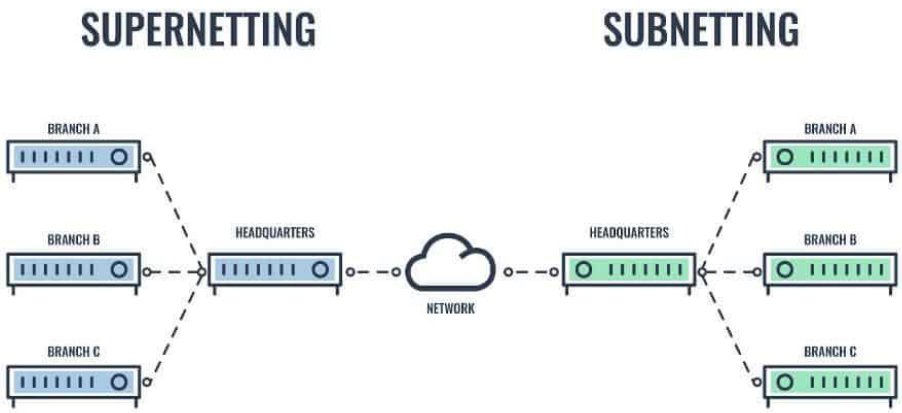

Figure 1 supernetting Vs. subnetting

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

Let's take an example:
A company called ABC needs to interconnect its 25 offices located around the World. In order to do that, it requires 25 public IP addresses that are requested to the ICANN. Without CIDR/VLSM, the obvious choice would be the use of a Class C address. By default, a Class C address offers 8 bits for the host part, so up to 254 devices can be uniquely identified and connected to the network.
The IP address block assigned by ICANN is the following: **195.1.1.0/24**
It's clear that the company needs to pay for 254 public IP addresses (range from 195.1.1.1 to 195.1.1.254) even though it is only using 25 of them. What happens to the remaining 232 IP addresses? Unluckily they are unused and no other organization can utilize them because already assigned to company XYZ. The wasting of addressing space is relevant and has economic implications (the public IP addresses are expensive) but also technical implications (wasting of IP addresses so accelerating the exhaustion).

The introduction of CIDR/VLSM allowed the allocation of a smaller block of IP addresses: **195.1.1.0/27**
The Subnet Mask was /24 (Class C) but is now /27 and that means 3 bits have been stolen to create the subnet field. The range of public IP assigned to the XYZ company is now from 195.1.1.1 to 195.1.1.30, a total of 30 IP addresses. This means having all 25 offices connected to the network, with a minimum waste of 5 IP addresses (while before it was 232).

Summarizing everything in a table:

	WITHOUT CIDR/VLSM (CLASSFUL)	**WITH CIDR/VLSM (CLASSLESS)**
IP Block Assigned	195.1.1.0/24	195.1.1.0/27
Number of Networks Available	1	1
Number of Hosts Available	254	30
Usable IP Range	da 195.1.1.1 a 195.1.1.254	da 195.1.1.1 a 195.1.1.30

From IPv4 to IPv6

As explained, VLSM and CIDR are two components of the same mechanism that allows an efficient partitioning of the IP addressing space. All modern networks work this way, and often the terms VLSM and CIDR are interchangeable. Besides the terminology, what is important is understanding how the introduction of the Subnet field allowed the IP Protocol to survive for 30 years of field use, avoiding wasting of addressing space that would have caused the IP exhaustion much earlier than that.

ARIN recently announced the exhaustion of free IPv4 addresses, so the IPv4 addressing space is now depleted. The IP protocol was first conceived in 1974 and presented in a paper entitled “A Protocol for Packet Network Intercommunication”. IP versions from 0 to 3 were experimental, used between 1977 and 1979. The following one, IP Version 4 (IPv4), is the one that we all know. Mechanisms like CIDR and VLSM allowed this network protocol to last 40+ years before running out of space.

Hence To summarize advantages of using VLSM and CIDR together in a single network:

- Efficient Address Space Allocation
- Elimination of Class Imbalances
- Efficient Routing Entries
- No Separate Subnetting Method
- Allows the use of multiple subnet mask lengths.
- Breaks up an address block into smaller custom blocks.
- Allows for route summarization.
- Provides more flexibility in network design.
- Supports hierarchical enterprise networks.

Question No. 2

Solution to Question No. 2:

IEEE 802.11 is part of the IEEE 802 set of local area network (LAN) protocols, and specifies the set of media access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) Wi-Fi computer communication in various frequencies including, but not limited to, 2.4 GHz, 5 GHz, 6 GHz, and 60 GHz frequency bands.

They are the world's most widely used wireless computer networking standards, used in most home and office networks to allow laptops, printers, smartphones, and other devices to communicate with each other and access the Internet without connecting wires. They are created and maintained by the Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee (IEEE 802).

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

Table 1 Description of 802.11a Wi-Fi Protocol

Description	• IEEE802.11a is the first wireless standard to employ packet based OFDM, based on a proposal from Richard van Nee from Lucent Technologies in Nieuwegein. • OFDM was adopted as a draft 802.11a standard in July 1998 after merging with an NTT proposal. It was ratified in 1999.
Data rate	• The maximum raw data rate of 54 Mbit/s, which yields realistic net achievable throughput in the mid-20 Mbit/s. • The data rate is reduced to 48, 36, 24, 18, 12, 9 then 6 Mbit/s if required. • For 20 MHz bandwidth, all the possible data rates are reduced to half. For 5/10 MHz, all possible data rates are reduced to $1/4^{th}$.
Bandwidth	5/10/20 MHz
Frequency bandwidth	5 GHz
Access techniques	Carrier Sensing Medium Access/ Collision Avoidance (CSMA/CA)
Modulation techniques	This uses Orthogonal frequency-division multiplexing (OFDM) to achieve Frequency Division Multiple Access (FDMA).

Table 2 Description of 802.11b Wi-Fi Protocol

Description	• 802.11b products appeared on the market in mid-1999. • It is used in a point-to-multipoint configuration, wherein an access point communicates via an omnidirectional antenna with mobile clients within the range of the access point.
Data rate	• 802.11b has a maximum raw data rate of 11 Mbit/s. • In practice the maximum 802.11b throughput that an application can achieve is about 5.9 Mbit/s using TCP and 7.1 Mbit/s using UDP. • It can also have values of 5.5,2 & 1 Mbit/s.
Bandwidth	22 MHz
Frequency bandwidth	2.4 GHz
Access techniques	It uses the same CSMA/CA media access method defined in the original standard.
Modulation techniques	• It is a direct extension of the DSSS (Direct-sequence spread spectrum) modulation technique defined in the original standard. • Technically, the 802.11b standard uses complementary code keying (CCK) as its modulation technique, which uses a specific set of length 8 complementary codes that was originally designed for OFDM but was also suitable for use in 802.11b because of its low autocorrelation properties.

Table 3 Description of 802.11g Wi-Fi Protocol

Description	• 802.11g is the third modulation standard for wireless LANs. • This specification under the marketing name of Wi-Fi has been implemented all over the world. • The 802.11g protocol is now Clause 19 of the published IEEE 802.11-2007 standard, and Clause 19 of the published IEEE 802.11-2012 standard.
Data rate	• It operates at a maximum raw data rate of 54 Mbit/s. • 31.4 Mbit/s is the maximum net throughput possible for packets of 1500 bytes in size and a 54 Mbit/s wireless rate. • In practice, access points may not have an ideal implementation and may therefore not be able to achieve even 31.4 Mbit/s throughput with 1500-byte packets. 1500 bytes is the usual limit for packets on the Internet and therefore a relevant size to benchmark against. • Smaller packets give even lower theoretical throughput, down to 3 Mbit/s using 54 Mbit/s rate and 64-byte packets.
Bandwidth	20 MHz
Frequency bandwidth	2.4 GHz
Access techniques	It uses the CSMA/CA transmission scheme
Modulation techniques	• The modulation scheme used in 802.11g is orthogonal frequency-division multiplexing (OFDM) copied from 802.11a with data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/s, and reverts to CCK (like the 802.11b standard) for 5.5 and 11 Mbit/s and DBPSK/DQPSK+DSSS for 1 and 2 Mbit/s. • Even though 802.11g operates in the same frequency band as 802.11b, it can achieve higher data rates because of its heritage to 802.11a.

Table 4 Description of 802.11n Wi-Fi Protocol

Description	• 802.11n is a wireless-networking standard that uses multiple antennas to increase data rates. • The Wi-Fi Alliance has also retroactively labelled the technology for the standard as Wi-Fi 4.
Data rate	• An 802.11n network can achieve 72 megabits per second (on a single 20 MHz channel with one antenna). • It can go up to 288 Mbit/s in 20 MHz mode with four antennas, or 600 megabits per second in 40 MHz mode with four antennas and 400 ns guard interval.
Bandwidth	20/40 MHz
Frequency bandwidth	It can be used in the 2.4 GHz or 5 GHz frequency bands
Access techniques	It uses the CSMA/CA transmission scheme.
Modulation techniques	MIMO-OFDM (multiple-input multiple-output- Orthogonal Frequency Division Multiplexing)

Table 5 Description of 802.11ac Wi-Fi Protocol

Description	• 802.11ac is a wireless networking standard in the 802.11 set of protocols, providing high-throughput wireless local area networks (WLANs) on the 5 GHz band. • The standard has been retroactively labelled as Wi-Fi 5 by Wi-Fi Alliance.
Data rate	• It can go up to 346.8 Mbit/s on 20MHz channel. • It can go up to 800 Mbit/s on 40Mz channel. • It can go up to 1.7 Gbit/ s on 80MHz channel, up to 3.4 Gbit/s on 160 MHz channel.
Bandwidth	20/40/80/160 MHz
Frequency bandwidth	5 GHz
Access techniques	It uses the CSMA/CA transmission scheme.
Modulation techniques	Multi user MIMO-OFDM

Table 6 Description of 802.11ax Wi-Fi Protocol

Description	• The 802.11ax standard is expected to be published in February 2021. • It is designed to operate in license exempt bands between 1 and 6 GHz when they become available for 802.11 use.
Data rate	• It can go up to 1.1 Gbit/s on 20MHz channel, • up to 2.2 Gbit/s on 40Mz channel, • up to 4.8 Gbit/ s on 80MHz channel, • up to 9.6 Gbit/s on 80+80 MHz channel.
Bandwidth	20/40/80/ 80+80 MHz
Frequency bandwidth	2.4/5/6 GHz
Access techniques	It uses the CSMA/CA transmission scheme.
Modulation techniques	Multi user MIMO-OFDM

2.2 Explain the different encryption techniques used in IEEE 802.11 Wi-Fi protocols.

2.2.1 Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 standard ratified in 1997, its intention was to provide data confidentiality comparable to that of a traditional wired network. WEP was the only encryption protocol available to 802.11a and 802.11b devices built before the WPA standard

WEP uses the stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity. It was deprecated in 2004.

2.2.2 RC4

RC4 generates a pseudorandom stream of bits (a keystream). These can be used for encryption by combining it with the plaintext using bit-wise exclusive-or; decryption is performed the same way. This is similar to the one-time pad except that generated pseudorandom bits, rather than a prepared stream, are used.

To generate the keystream, the cipher makes use of a secret internal state which consists of two parts:

- A permutation of all 256 possible bytes (denoted "S" below).
- Two 8-bit index-pointers (denoted *"i"* and *"j"*).

The permutation is initialized with a variable length key, typically between 40 and 2048 bits, using the key-scheduling algorithm (KSA). Once this has been completed, the stream of bits is generated using the pseudo-random generation algorithm (PRGA)

Pseudo codes

the key-scheduling algorithm (KSA)

```
for i from 0 to 255
    S[i] := i
endfor
j := 0
for i from 0 to 255
    j := (j + S[i] + key[i mod keylength]) mod 256
    swap values of S[i] and S[j]
endfor
```

pseudo-random generation algorithm (PRGA)

```
i := 0
j := 0
while GeneratingOutput:
    i := (i + 1) mod 256
    j := (j + S[i]) mod 256
    swap values of S[i] and S[j]
    K := S[(S[i] + S[j]) mod 256]
    output K
endwhile
```

Security of RC4:

Unlike a modern stream, RC4 does not take a separate nonce alongside the key. This means that if a single long-term key is to be used to securely encrypt multiple streams, the protocol must specify how to combine the nonce and the long-term key to generate the stream key for RC4. One approach to addressing this is to generate a "fresh" RC4 key by hashing a long-term key with a nonce. However, many applications that use RC4 simply concatenate key and nonce; RC4's weak key schedule then gives rise to related key attacks, like the Fluhrer, Mantin and Shamir attack (which is famous for breaking the WEP standard).

2.2.3 Wi-Fi Protected Access (WPA)

The Wi-Fi Alliance intended WPA as an intermediate measure to take the place of WEP pending the availability of the full IEEE 802.11i standard. WPA could be implemented through firmware upgrades on wireless network interface cards designed for WEP that began shipping as far back as 1999.

The WPA protocol implements much of the IEEE 802.11i standard. Specifically, the Temporal Key Integrity Protocol (TKIP) was adopted for WPA. WEP used a 64-bit or 128-bit encryption key that must be manually entered on wireless access points and devices and does not change. TKIP employs a per-packet key, meaning that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP.

TKIP and the related WPA standard implement three new security features to address security problems encountered in WEP protected networks. First, TKIP implements a key mixing function that combines the secret root key with the initialization vector before passing it to the RC4 cipher initialization. WEP, in comparison, merely concatenated the initialization vector to the root key, and passed this value to the RC4 routine. This permitted the vast majority of the RC4 based WEP related key attacks. Second, WPA implements a sequence counter to protect against replay attacks. Packets received out of order will be

rejected by the access point. Finally, TKIP implements a 64-bit Message Integrity Check (MIC) and re-initializes the sequence number each time when a new key (Temporal Key) is used.

To be able to run on legacy WEP hardware with minor upgrades, TKIP uses RC4 as its cipher. TKIP also provides a rekeying mechanism. TKIP ensures that every data packet is sent with a unique encryption key (Interim Key/Temporal Key + Packet Sequence Counter)

Security

TKIP uses the same underlying mechanism as WEP, and consequently is vulnerable to a number of similar attacks. The message integrity check, per-packet key hashing, broadcast key rotation, and a sequence counter discourage many attacks. The key mixing function also eliminates the WEP key recovery attacks.

Notwithstanding these changes, the weakness of some of these additions have allowed for new, although narrower, attacks like packet spoofing, etc.

2.2.4 Wi-Fi Protected Access II (WPA2)

Ratified in 2004, WPA2 replaced WPA. WPA2, which requires testing and certification by the Wi-Fi Alliance, implements the mandatory elements of IEEE 802.11i. In particular, it includes mandatory support for CCMP, an AES-based encryption mode.

Counter Mode Cipher Block Chaining Message Authentication Code Protocol (Counter Mode CBC-MAC Protocol) or CCM mode Protocol (CCMP) is an encryption protocol designed for Wireless LAN, it is an enhanced data cryptographic encapsulation mechanism designed for data confidentiality and based upon the Counter Mode with CBC-MAC (CCM mode) of the Advanced Encryption Standard (AES) standard. It was created to address the vulnerabilities presented by Wired Equivalent Privacy (WEP)

CCMP uses CCM that combines CTR mode for data confidentiality and CBC-MAC for authentication and integrity. CCMP is based on AES processing and uses a 128-bit key and a 128-bit block size.

AES is based on a design principle known as a substitution–permutation network, and is efficient in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael, with a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits.

High-level description of the algorithm

1. **KeyExpansion**: round keys are derived from the cipher key using the AES key schedule. AES requires a separate 128-bit round key block for each round plus one more.
2. Initial round key addition:
    - **AddRoundKey**: each byte of the state is combined with a byte of the round key using bitwise XOR.
3. 9, 11 or 13 rounds:
    - **SubBytes**: a non-linear substitution step where each byte is replaced with another according to a lookup table.
    - **ShiftRows**: a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
    - **MixColumns**: a linear mixing operation which operates on the columns of the state, combining the four bytes in each column.
    - **AddRoundKey**
4. Final round (making 10, 12 or 14 rounds in total):
    - **SubBytes**
    - **ShiftRows**
    - **AddRoundKey**

Security

CCMP is much more secure than the Wired Equivalent Privacy (WEP) protocol and Temporal Key Integrity Protocol (TKIP) of Wi-Fi Protected Access (WPA). CCMP provides the following security services:

- Data confidentiality; ensures only authorized parties can access the information
- Authentication; provides proof of genuineness of the user
- Access control in conjunction with layer management

Because CCMP is a block cipher mode using a 128-bit key, it is secure against attacks to the 2^{64} steps of operation. Generic meet-in-the-middle attacks do exist and can be used to limit the theoretical strength of the key to $2^{n/2}$ (where n is the number of bits in the key) operations needed.

2.2.5 Wi-Fi Protected Access 3 (**WPA3**)

In January 2018, the Wi-Fi Alliance announced WPA3 as a replacement to WPA2. The new standard uses an equivalent 192-bit cryptographic strength in WPA3-Enterprise mode (AES-256 in GCM mode with SHA-384 as HMAC), and still mandates the use of CCMP-128 (AES-128 in CCM mode) as the minimum encryption algorithm in WPA3-Personal mode.

The WPA3 standard also replaces the Pre-Shared Key exchange with Simultaneous Authentication of Equals as defined in IEEE 802.11-2016 resulting in a more secure initial key exchange in personal mode and forward secrecy. The Wi-Fi Alliance also claims that WPA3 will mitigate security issues posed by weak passwords and simplify the process of setting up devices with no display interface.

Bibliography

1. https://techdifferences.com/difference-between-cidr-and-vlsm.html
2. https://en.wikipedia.org/wiki/IEEE_802.11
3. https://www.ccexpert.us/ospf-network/explaining-the-need-for-vlsm-and-cidr.html
4. https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy