IEEE 802.11 wireless LAN Security

* There are two principal types of WLANs
* Adhoc networks, where stations communicate directly with each other.
* Infrastructure WLANs, which use an access point.
* A station first sends a frame to an AP and the AP then delivers it to its final destination.
* The destination may be another wireless station. Alternatively, it may be a station on the wired network that the AP is connected to.
* The AP thus serves as a bridge b/w the WLAN & the existing wired n/w.
* A n/w of wireless stations associated with an AP is referred to as a basic service set. Such a n/w may be adequate for a home or small enterprise.
* In a large building or campus all stations may not fall in the range of a single AP. It'll be necessary to have several APs to cater to the stations dispersed over a set of buildings. For example: The APs in the different basic service sets are often connected over a wired n/w.

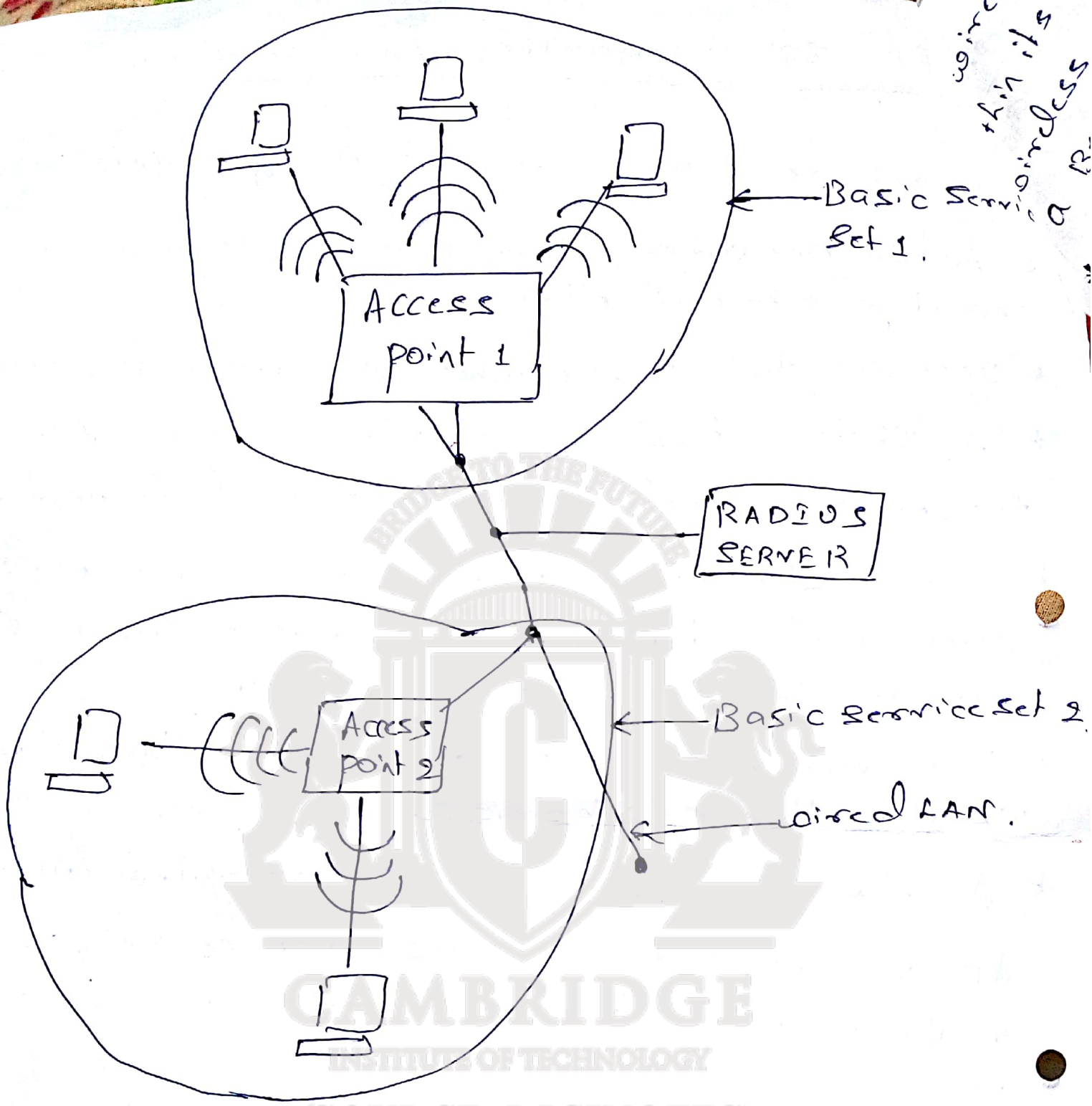


Fig:- Infrastructure wireless LAN.

* The union of the basic service sets comprises an extended service set (ESS).
* Each station and AP in the ESS is uniquely identified by a MAC address - a 48-bit quantity.
* Each AP is also identified by an SSID (service Set ID), which is a character string of length at most 32 characters.

wireless station, needs to first discover an AP within its range. This can be done by monitoring the wireless medium for a special kind of frame called a Beacon, which is periodically broadcast by the AP.

* The Beacon usually contains the SSID of the broadcasting AP.

* Alternatively a station may send a probe Request frame. An AP, on hearing such a request, responds with a probe Response frame. The probe Response frame contains the SSID of the AP and also information about its capabilities, supported data rates etc.

* To become part of the WLAN, a station will have to associate with an AP. At any point in time a station can associate with only one AP.

* A Station that wishes to associate with an AP sends it an Associate Request frame. The AP replies with an Associate Response frame if it accepts the request for associating with it.

AUTHENTICATION.

1. pre-WEP Authentication.

* knowledge of the SSID sufficed for a station to be authenticated to the AP.

* However, an attacker could easily sniff the value of SSID from frames such as the beacon or probe response & then use it for authentication.

* Another approach was to restrict admission to the WLAN by MAC address. The AP would maintain a list of MAC addresses of stations permitted to join the WLAN.

* valid MAC addresses could be obtained by sniffing the wireless medium. The attacker could then modify his n/w card to spoof a valid MAC address. So neither of these approaches helped.

2. Authentication in WEP.

* The station authenticates itself to the AP using a challenge-response protocol.
* The AP generates a challenge (nonce) and sends it to the station.
* The station encrypts the challenge and sends it to the AP.
* The stream cipher, RC4 is used for encryption.
* The station computes a keystream, which is a function of a 40-bit shared secret s and a 24-bit IV.
* The challenge is then XORed with the keystream to create the response.

RESPONSE = CHALLENGE ⊕ KEYSTREAM(S, IV)

* All an attacker needs to do is to monitor a challenge-response pair. From this, he can compute the keystream. To authenticate himself to the AP, he needs to XOR the challenge from the AP with the computed keystream.

* It may also be possible for an attacker to obtain S itself. By eavesdropping on several challenge-response pairs b/w the AP and various stations, an attacker could launch a dictionary attack & eventually obtain S.

* Note: There is no support for authenticating the AP to a station, so door to man-in-the-middle attacks

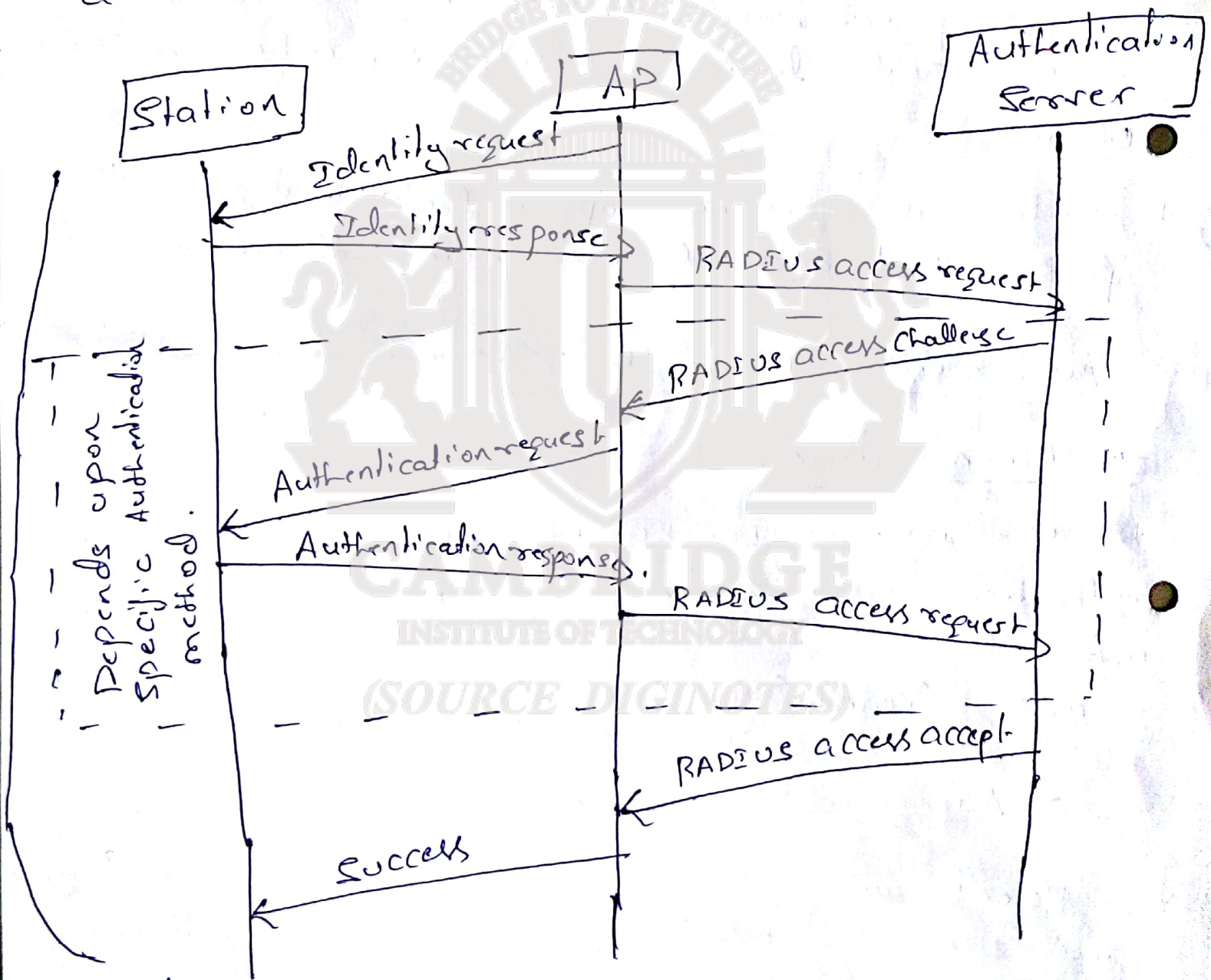
3. Authentication and key Agreement in 802.11i.

a. Authentication.

* 802.11i uses IEEE 802.1x - a protocol that supports authentication at the link layer. Three entities are involved:
  a. Supplicant (the wireless station)
  b. Authenticator (the AP)
  c. Authentication server.

* Different authentication mechanisms and message types are defined by IETF's Extensible Authentication protocol (EAP).

* EAP is not really an authentication protocol but rather a framework upon which various authentication protocols may be supported.
* EAP exchanges are mainly comprised of requests and responses.
* The Generic authentication messages in IEEE 802.11i are shown below.



EAPOL = EAP over LANs
EAP = Extensible Authentication protocol.

Fig:- Authentication and master session key exchange in 802.11i

* The protocol used b/w the station and the Ap is EAP but that used b/w the Ap & the AS depends upon the specifics.

* AS is often a RADIUS Server which uses its own message types & formats.

* RADIUS Stands for Remote authentication Dial in User Service. It is a client-Server protocol used for authentication, authorization and accounting.

- The main authentication methods supported by EAP include the following:

  EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP.

* EAP-MD5: The most basic of the EAP authentication methods.

1. The authentication Server challenges the station to transmit the MD5 hash of the user's password
2. The Station prompts the user to type his/her password. It then computes the hash of the password & sends this across.
3. Attacker could eavesdrop on such a msg exchange and then replay the hashed password thus impersonating the owner of the password. This method does not support authentication of the Ap to the Station.

* EAP-TLS: 1) It is the most secure and provides mutual authentication and agreement on a master session key.

2) It requires the AP as well as the user (station) to have digital certificates.

3) It is relatively straightforward to equip each AP with a DC and a corresponding private key but extending the PKI to each user of the WLAN may not be feasible.

* EAP-TTLS:

1) It requires certificates only at the AP end.

2) The AP authenticates itself to the station & both sides construct a secure tunnel b/w themselves.

3) over this secure tunnel, the station authenticates itself to the AP.

4) The station could transmit attribute-value pairs such as

user_name = ramesh

password = 4rp#mNaS27

5) note: the station really authenticates itself to the RADIUS server - the AP merely forwards the authentication information to the RADIUS server.

* EAP-protected EAP (PEAP):

1) In PEAP, the secure tunnel is used to start a second EAP exchange wherein the station authenticates itself to the authentication server.

b. Key Hierarchy.

* Two types of keys used in WLANs.

1) pairwise keys: used to protect traffic between a station and an AP.

2) Group key: used to protect broadcast or multicast traffic between an AP and multiple stations.

* The root of the key hierarchy is the pairwise master key (PMK). This is obtained in one of two ways.

1) MSK [Master session key]

2) PSK [pre-shared key]

MSK: The station and the authentication server may agree on a MSK. The authentication server then communicates this key to the AP. The AP and station then derive the PMK from the MSK.

PSK: An alternative to computing a fresh PMK for each session is the pre-shared key (PSK), which is used as the PMK.

* The 256-bit PMK is used to derive a 384-bit pairwise Transient key (PTK).

* PTK is a pseudorandom function of the PMK, two nonces chosen by the AP, and the station and their MAC addresses.

* By deriving the PTK in this fashion, key refreshing can take place without the overhead of negotiating a new PMK.

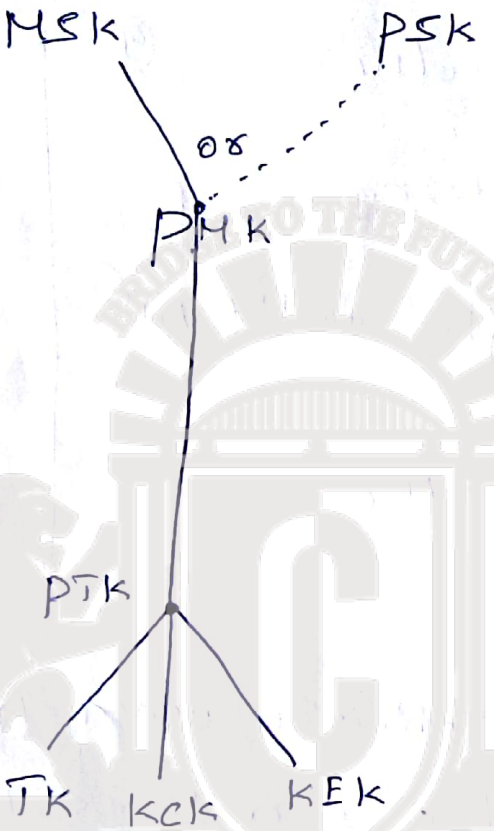
* Three 128-bit chunks are extracted from the 384-bit PTK for the following purposes:

1) A Temporal key (TK) It is used for both encryption and integrity protection of data between the AP and the station.

2) A key confirmation key (KCK): It is used to integrity-protect some of the messages in the four-way handshake. Integrity protection is supported by a MAC computed as a function of the message and the KCK.

3) A key Encryption key: It is used to encrypt the message containing the group key.

*Figure: The key hierarchy in 802.11i is Summari



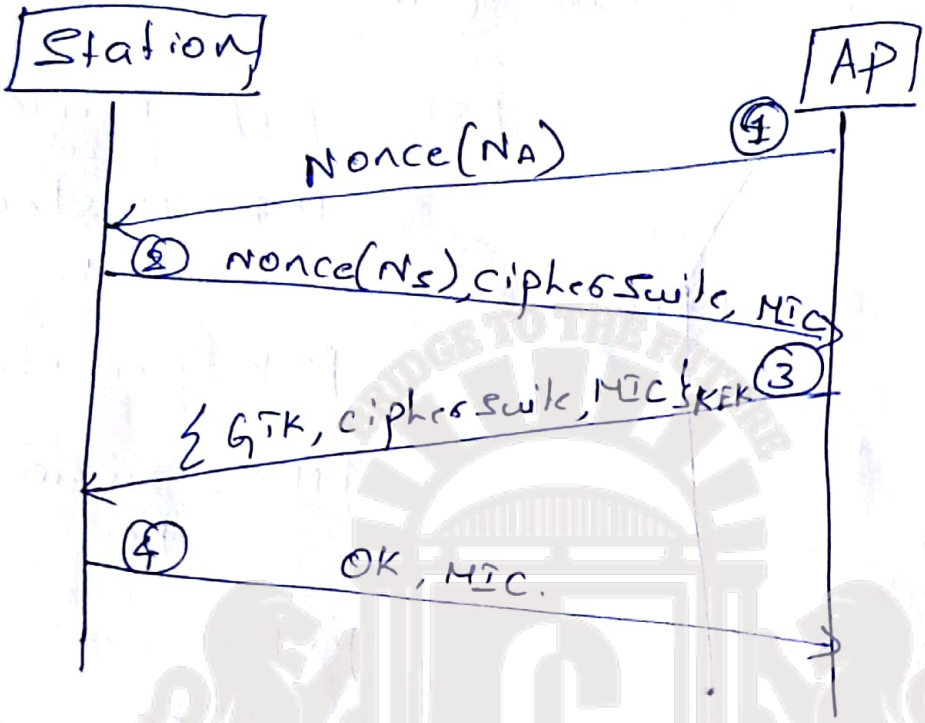
KEK = key confirmation key.
MSK = Master session key.
PSK = pre-shared key
PMK = pairwise Master key.
PTK = pairwise transient key.
TK = Temporal key.
KCK = key confirmation key.

Four-way handshake.

* The main goals of the four-way handshake are to

1) derive the PTK from the PMK.
2) verify the cipher suites communicated in the Beacon and associate Request frames and
3) communicate the group keys from the AP to the Station.

* Figure: Shows the messages comprising the four-way handshake.



1. The AP first sends a nonce, N_A, to the station.
2. The station chooses a nonce, N_S. The station computes the PTK as follows

$$PTK = PRF(PMK, N_A, N_S, MAC_A, MAC_S)$$

The station sends its nonce together with its choice of cipher suite to the AP. It uses the KCK to compute a msg integrity check (MIC). Such protection thwarts a possible man-in-the middle attack intended to replace cryptographic algorithms in the cipher suite for possibly weaker options.

On receiving the msg containing N_S, the AP computes the PTK from the expression used by the station.

It then extracts TK, KCK, and KEK. In addition, the AP verifies the integrity and source of Msg2 using the key, KCK.

3. Msg 3 from the AP to the Station contains the current Group transient key (GTK). This is the key used by the AP and all Stations to integrity protect all multicast or broadcast msges. Msg 3 also contains the cipher suite chosen by the AP. The msg is encrypted using the KEK and is integrity protected using KCK.

4. Msg 4 is an acknowledgement from the Station that it has received the previous msges without error. It is a signal to the AP that henceforth all messages ll be integrity-protected and encrypted with the TK.

Confidentiality and Integrity

Data protection in WEP

* It is designed to provide msg confidentiality Integrity and access control but it failed on all three counts.
*

WEP encryption and Integrity checking

* WEP uses the Stream cipher, RC4, for encrypting messages.
* It generates a pseudo-random keystream ks, which is a function of secret shared b/w the two communicating parties.
* In order to have ks vary from msg to msg, a random per-msg initialization vector IV, is also used to generate ks.
* ks is ⊕ed with the plaintext p, to obtain the ciphertext c or

$$c = p \oplus ks(s, IV) \quad \text{---} (1)$$

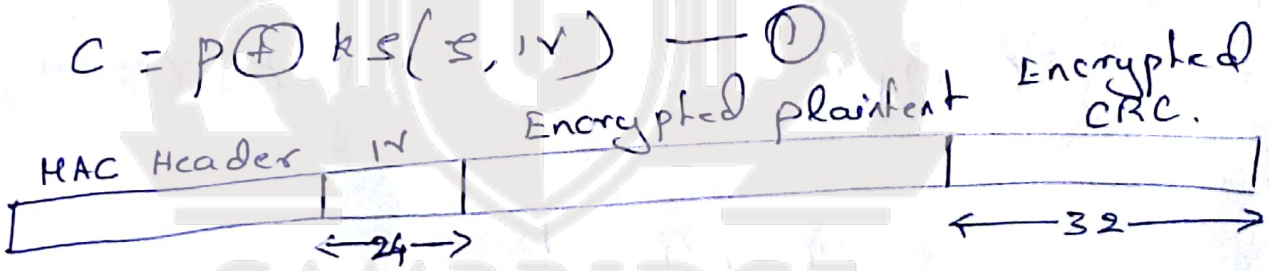


Fig: WEP frame.

* 32-bit CRC checksum computed on the msg, and encryption performed on plaintext & CRC using RC4, the IV chosen by the sender is included in each frame.
* To decrypt the msg, the receiver generates ks from the shared secret s, and the IV retrieved from the received frame. It recovers the plaintext from the following equation

$$p = c \oplus ks(s, IV)$$

known plaintext Attack.

* The first problem with WEP is the possibility of keystream re-use.
* Since the IV is 24 bits in length, there are only 2^{24} distinct keystreams that could be constructed given a secret S.
* Suppose an attacker finds two frames which were encrypted using the same IV.
* Let their ciphertexts be C & C'. Let the corresponding plaintexts be P & P'.
* using equation 1, it follows that

$$P \oplus P' = C \oplus C'$$

so

$$P' = P \oplus C \oplus C'$$

knowing C, C' & P we can obtain P'.

Msg modification.

* The sender's plaintext be $M_1 F M_2$ where M_1, F & M_2 are each binary strings.
* The attacker wishes to substitute the substring F, with another substring F', so that the decrypted msg seen by the receiver is $M_1 F' M_2$.

* The msg integrity check should detect any modification to an existing msg.

* The ciphertext computed by the sender is

$$((M_1 F M_2) \| CRC(M_1 F M_2)) \oplus ks.$$

* The attacker intercepts the ciphertext and performs the following operations:

1. He first constructs the string.
2. He then computes the CRC on this string.
3. He finally XORs the original ciphertext with the constructed string.

* The computation yield.

$$((M_1 F' M_2) \| CRC(M_1 F' M_2)) \oplus ks$$

* The last step follows from the fact that the CRC is a linear operation i.e.

$$CRC(m_1 \oplus m_2) = CRC(m_1) \oplus CRC(m_2)$$

* The receiver, on decrypting the ciphertext, obtains

$$(M_1 F' M_2) \| CRC(M_1 F' M_2)$$

* The modified msg has a valid CRC & so passes the integrity check at the receiver. Hence the receiver accepts the msg, unaware that it has been modified by an attacker.

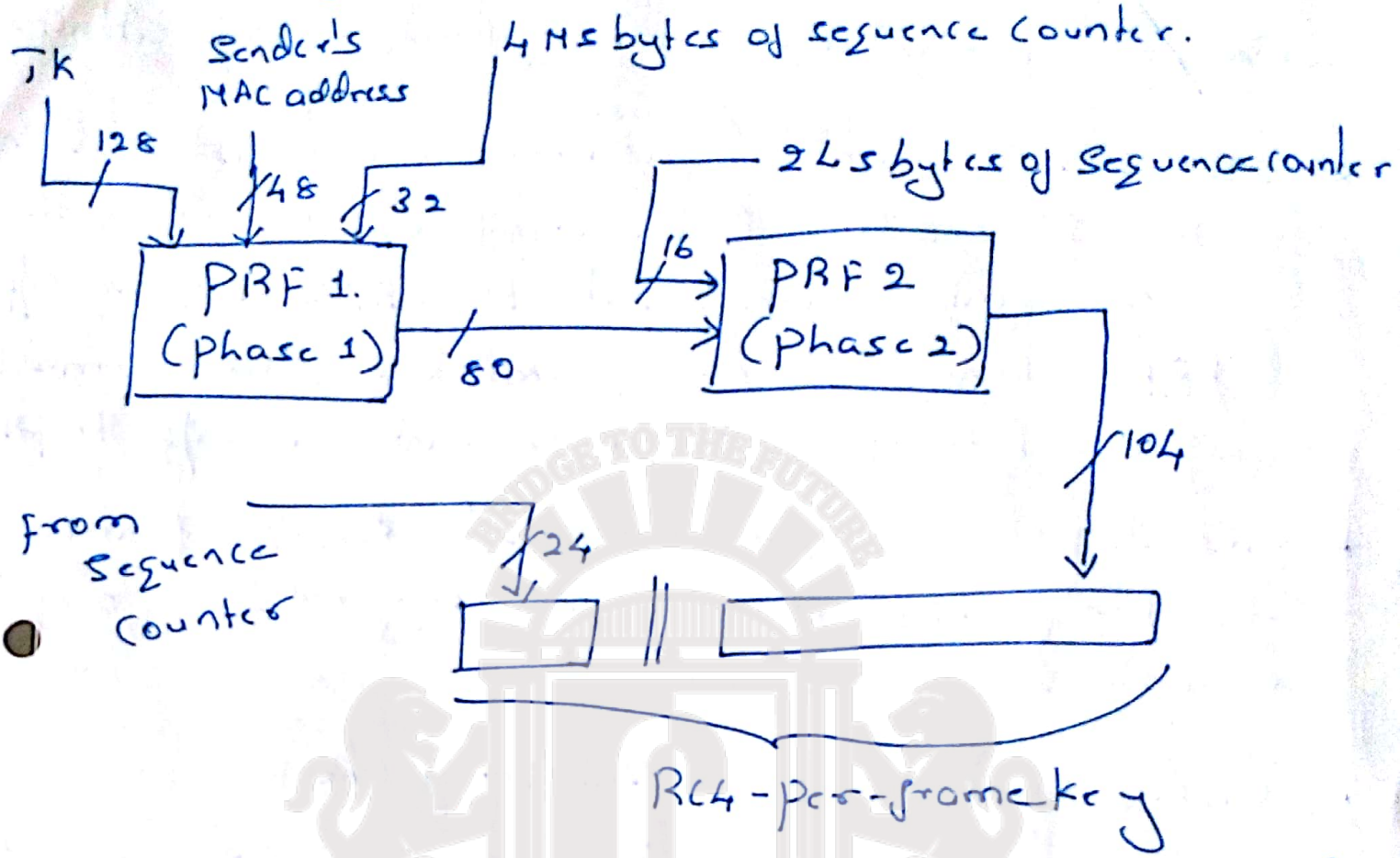
Data protection in TKIP and CCMP.

* There are many more attacks on RC4 as used in WEP.
* A well-known example is the FMS attack named after Fluhrer, Mantin and Shamir.
  1. By collecting a sufficient no of frames over the air bearing specific IVs, the encryption key used in WEP can be deduced.
* Soln for easily Weakness are wireless protected Access (WPA), the technical name for WPA is Temporal Key Integrity protocol (TKIP) and counter Mode with CBC MAC protocol (CCMP) (uses AES).

TKIP.

*. The problem is that the variable part of the WEP key is too small, so the per-frame keystream repeats frequently.
+ In TKIP, the encryption key in TKIP is 128 bits, so there was much randomness in most of the 128 bits of the key and that the probability of keystream collisions was negligible.
+ TKIP Generates a random and different encryption key for each frame sent.

* It employs a process called two-phase key mixing



* The inputs to this process are the 128-bit temporal key, TK, the sender's MAC address and the 4 most significant bytes of a 48-bit frame sequence counter.

* The randomizing capabilities of the key mixing function and the large size of the key space virtually guarantee that "keystream collisions" never occur. Thus, known plaintext attacks that could be successfully launched on WEP have no chance of success with TKIP.

* The sequence counter is incremented for each frame sent. It is also carried in the header of each frame. It is extracted by the receiver and used to compute the RC4 key for decryption. Both sender and receiver keep track of the sequence no of the last frame sent/received. The receiver accepts a fresh frame only if the

frame's sequence no is greater than that of the previous frame received from the same sender. This helps protect the receiver from replay attacks.

* Two pseudo-random functions are employed in the two phases. The least significant 16 bits of the sequence counters are inputs to PRF2. So, the o/p of PRF2 changes for each frame sent. The 32 most significant bits of the sequence counter are i/p to PRF1
* This i/p changes after every $2^{16} = 65,536$ frames sent. Hence, PRF1 is executed very rarely & overall computation time is saved.

* CRC checksum as an integrity check.
* The 64-bit msg integrity check in TKIP, called MIC
  MIC is non-linear i.e

$$MIC(m_1 \oplus m_2) \neq MIC(m_1) \oplus MIC(m_2)$$

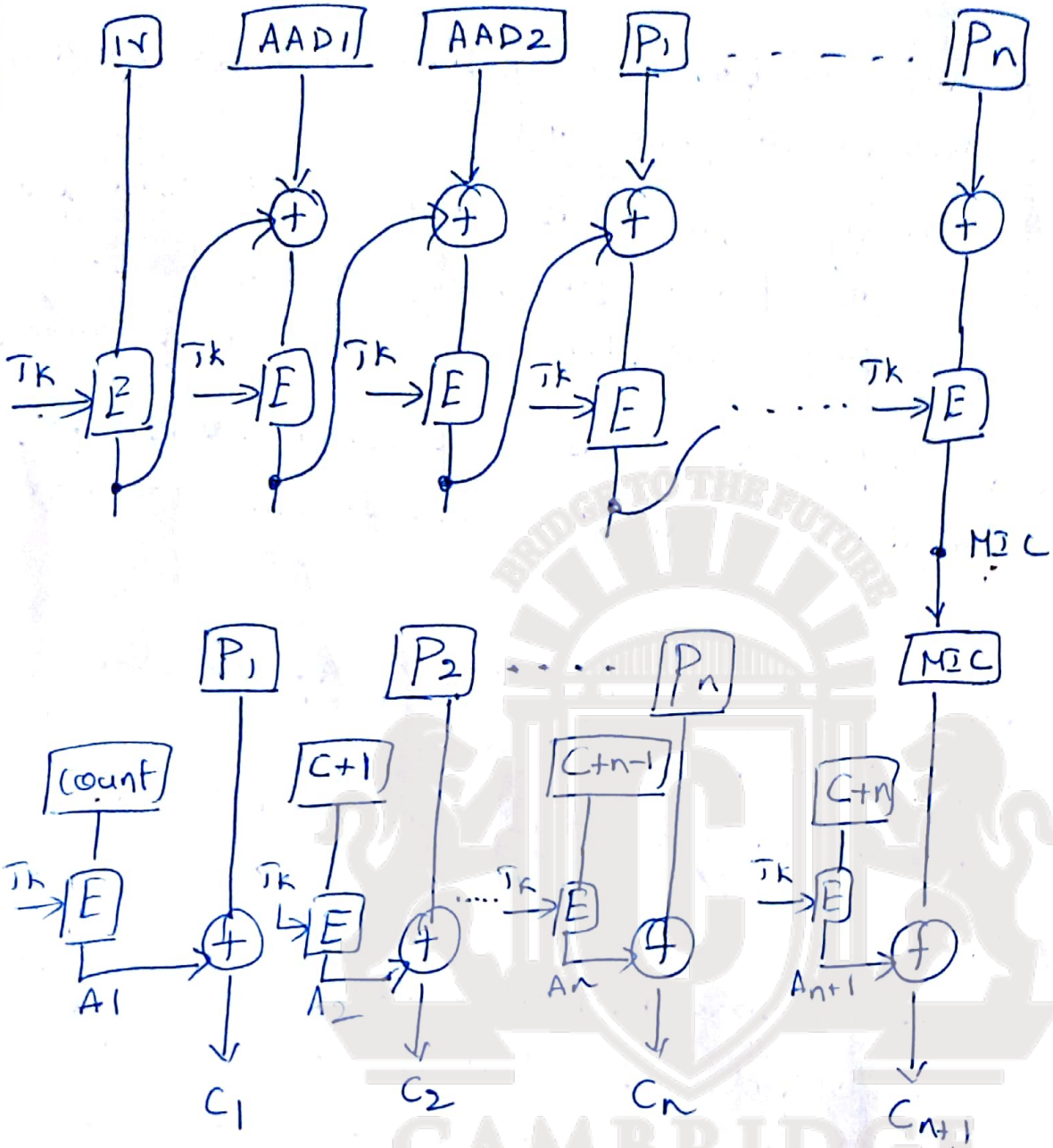
* MIC is computed as a function of the data in the frame and also some fields in the MA header such as the source and destination addresses. It also uses as i/p a key derived from the PTK.

* Due to design constraints on WEP cards, MIC's implementation uses simple logical functions & shifts etc Hence, it is not as secure as a keyed Cryptographic hash.

CCMP

* It uses the AES for both encryption and for providing msg source authentication/integrity.
* AES is a block cipher, there is no need to re-compute a fresh key for each frame, so the 128-bit temporal key, TK is used for encryption and MAC computation.
* The count is referred to as a packet number (PN). The count is maintained at both sender and receiver ends.
* The PN is included in a special CCMP header field in a CCMP frame.
* The PN is incremented by the sender after each frame is sent.
* Receipt of a fresh frame in that session, the receiver compares the value of PN in the CCM header versus the value stored by it. If the former is less than the stored value, the frame is likely to be a replayed frame and is hence discarded.
* The first task in preparing a frame for transmission is to compute a MIC.
* MIC is the frame data & several immutable fields in the MAC header.
* MIC is computed using AES in cipher block chaining (CBC) mode with block size = 128 bits.

Fig:- MAC Generation and encryption in CCMP.



IV = initialization vector (includes 48-bit packet no)

AAD1, AAD2 = Additional Authentication Data (includes certain immutable fields of the MAC header)

COUNT is a function of the packet no.

* The key for performing encryption in each stage is TK.

*. The IV for the MIC computation is a nonce, which includes the 48-bit PN.

* The second & third blocks used in the MIC computation are specific fields in the frame header such as the MAC addresses, sequence control & frame type.
* The blocks in the frame data are sequentially processed resulting in an 8-byte MIC.

* . Encryption:

1. The frame data and the MIC are concatenated and then encrypted using AES in countermode
2. Let n be the total no of blocks in the frame body + MIC.
3. The procedure for encrypting the i-th block is
   a. compute $A_i = E_{TK}(pn + i * j)$. Here, pn is the packet number and j is a constant known to both sender and receiver.
   b. compute i-th block of ciphertext = $A_i \oplus P_i$.
   Here P_i is the i-th block of plaintext.
4. The frame now includes two new fields - the CCMP header and the MIC.
5. upon receipt of the frame, the receiver reverses the operations performed by the sender. It performs decryption followed by MIC verification.

Firewalls

1. BASICS

1.1. Firewall functionality

* The main functions of a firewall are listed as follows

a. Access control: A firewall filters incoming (from the Internet into the organization) as well as outgoing (from within the organization to the outside) packets
A firewall is said to be configured with a ruleset based on which it decides which packets are to be allowed and which are to be dropped.

b. Address / port translation.

* NAT was initially devised to alleviate the serious shortage of IP addresses by providing a set of private addresses that could be used by system administrators on their internal n/w but that are globally invalid.
* publicly accessible m/c within an organization, such as web servers, may or may not have public Internet addresses.
* It is possible to conceal the addressing schema of these m/c from the outside world through the use of NAT. NATing is often done by firewalls

c. Logging

* In the process of filtering internet traffic, all

firewalls have some type of logging feature that documents how the firewall handled various types of traffic.

* It are very useful for studying attempts at intrusion together with various worm and DDoS attacks.

Authentication, caching:

* Some types of firewalls perform authentication of external machines attempting to establish a connection with an internal m/c.
* A special type of firewall called a web proxy authenticates internal users attempting to access an external service.
* web proxy firewall also used to cache frequently requested webpages. This results in decreased response time to the client while saving communication bandwidth

2. Policies and Access control lists

High level policies for access to various types of services

1. All received email should be filtered for spam & viruses.
2. All HTTP requests by external clients for access to authorized pages of the organizations website should be permitted.
3. The organizations employees should be allowed to remotely log into authorized internal machines. However all such communication should be authenticated and encrypted.

4. only two types of outgoing traffic are permitted. First, all e-mail from within the organization to the outside world are permitted. Second, requests from within the organization for external webpages are permitted.

5. DNS queries made by external clients should be allowed provided they pertain to addresses of the organization's publicly accessible services such as the web server or the external e-mail server.

* High-level policies are translated into a set of rules that comprise an ACL.

1. The packet's source IP address and port number.
2. The packet's destination IP address and port no.
3. The Transport protocol in use (TCP or UDP)
4. The packet direction - incoming or outgoing.

NO	(I) or (O)	Transport protocol	SIP addr	Src port.	Dest. IP add.	Dest port	Action	comment
1.	I	TCP	ANY	ANY	MS	25	permit	Allow incoming e-mail.
2.	I	TCP	ANY	ANY	WS	80	permit	Allow requests for organizations webpages
3.	I	UDP	ANY	ANY	NS	53	permit	Allow DNS queries
4.	I	IPsec	ANY	ANY	*	*	permit	Allow incoming vpn traffic.
5	I	ANY	ANY	ANY	ANY	ANY	Deny	Deny all other incoming traffic.
6.	O	TCP	ANY	ANY	ANY	25	permit	Allow outgoing email.
7.	O	TCP	"	"	*	80	permit	Allow requests for external webpages

5. 0 Any Any Any Any Any Deny. Deny all other outgoing traffic

* Two types of policy.
  1. permissive policy: permit all packets except those that are explicitly forbidden.
  2. Restrictive policy: Drop all packets except those that are explicitly permitted.

3. Firewall types.

1. packet filters and stateful inspection

* processing the ruleset involves checking from matches in the IP, TCP or UDP headers.
* for example it may be necessary to check whether a packet carries a certain specific source or destination IP address or port no.
* The earliest firewall designed to perform this task was referred to as a packet filtering firewall.
* It is often performed by the border router or access router that connects the organization's network to the Internet.
* The border router becomes the first line of defence against malicious incoming packets.

* Consider an external MS (IP = ABC) that wishes to deliver mail to an organization. For this purpose, it should first establish a TCP connection with the organization's mail server. SIPAdd = ABC, Dest = MS TCP Destination port = 25 ACK flag set
* Suppose such a connection has not yet been established Should the packet still be allowed in?
* The simple packet filter will allow the packet to enter even if no prior connection b/w ABC & MS was established Hence it will not be able to filter out such packets arriving from ABC.
* Stateful packet inspection firewall: It uses a packet's TCP flags and sequence/acknowledgement no to determine whether it is part of an existing, authorized flow.
* If it is participating in the establishment of an authorized connection or if it is already part of an existing connection, the packet is permitted, otherwise it is dropped.

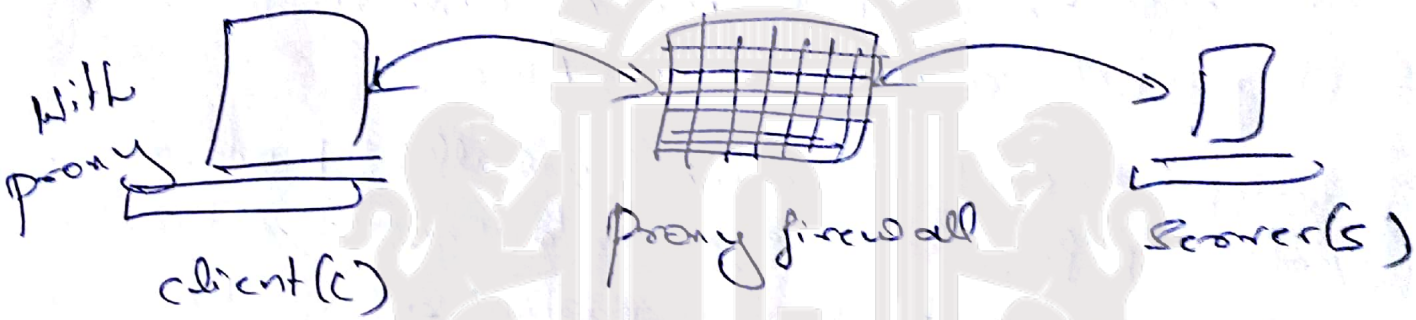
2. Application level firewalls.

* A packet-filtering firewall, even with the added functionality of stateful packet inspection, is still severely limited.
* It understands the n/w & transport layer headers
* needed is a firewall that can examine the application payload and scan packets for worms

viruses, spam mail & inappropriate content. such device is called a deep inspection firewall.

Fig:- proxy firewall.

Direct TCP connection b/w C & S.



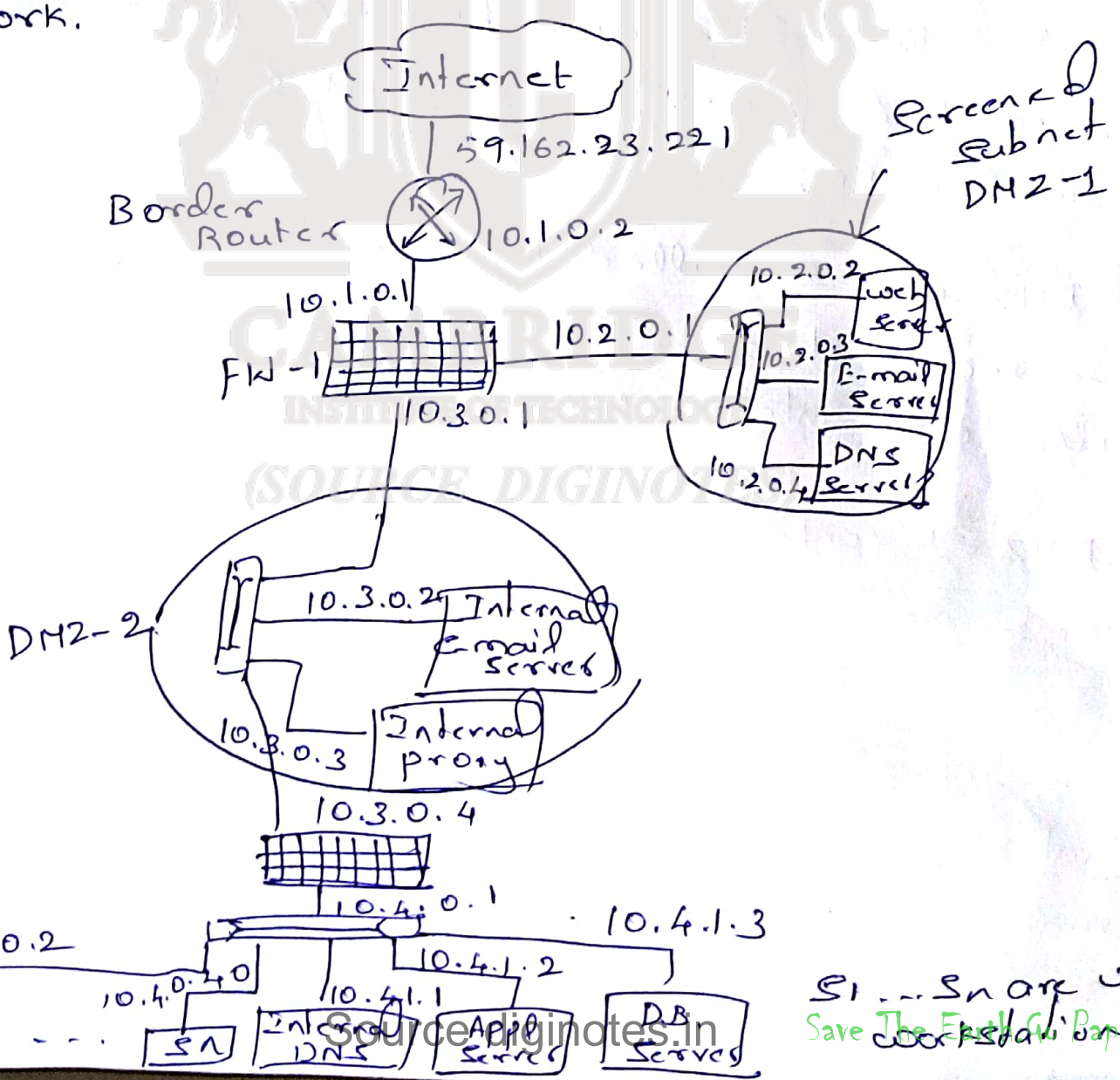
Two TCP connections b/w C & proxy & b/w proxy & S.

* There are proxy agents for many application layer protocols includes HTTP, SMTP & FTP.
* In addition to filtering based on application layer data, proxies can perform client authentication & logging.
* HTTP proxy can also cache webpages.
* Caching has a major impact on performance.

PRACTICAL ISSUES.

1. placement of firewalls.

* Firewalls help segregate or isolate the nlw into multiple security zones.
* Each firewall in the organization enforces rules that control the transfer of packets between different security zones.
* There are three zones - the internet, the region containing the publicly accessible servers and the internal network.
*



* Fig: depicts a four-zone layout using three firewalls.
* Border Router with some packet-filtering capability This is the access router that interfaces with the Internet. It is connected to a stateful firewall, FW-1, which has three interfaces.
* Firewalls that have more than two interfaces are referred to as multi-homed.
* The zone connected to the right interface of FW-1 referred to as a Screened subnet or De-Militalized zone(DMZ).
* A DMZ, is the area b/w two firewalls. The zone b/w firewalls FW-1 & FW-2 is a real DMZ labelled DMZ-2.
* DMZ are so called because they often host Servers that are accessible to the Internet & also to the internal nlw.
* DMZ-1 contains the publicly accessible Servers, These include the web Server, the external e-mail Server & the DNS Server. All incoming mail from the Internet is received by this e-mail Server, which checks for virus Signatures and Spam mail. The DNS Server resolves names of publicly accessible Servers.

* DMZ-2 contains the internal e-mail server. This is the server that hosts the mailboxes of the company employees. It handles the sending and receiving of all mail b/w internal pcs. It periodically establishes a connection to the external mail server (in DMZ-1) to retrieve all incoming mail. Outgoing mail (from the internal n/w to the internet) can be handled in several ways. The internal mail server can set up an SMTP connection to a remote mail server to transfer mail. Alternatively, it can connect to the external mail server (in DMZ-1) & use it to relay all outgoing mail.

* DMZ-2 also contains an Internet proxy server. All internal users who wish to access external webpages connect to the proxy. The proxy authenticates the internal user & decides whether a page can be accessed. The proxy scans incoming webpages for virus signatures & objectionable content. Finally, the proxy also performs caching of webpages.

* Internal n/w contains application servers, database servers, the user workstations. It also has an internal DNS server. This DNS server is different from the external DNS server in that it provides

mapping b/w the domain names of the internal mlcs & their IP addresses.

Firewall configuration.

Table: Simplified ruleset for firewall, FW-2.

NO	From IP Addr.	From port	TO IP Addr.	TO port	protocol	Action
1	*	*	Internal	*	*	Drop
2.	User	*	Int_Mail-S	25	SMTP	Accept
3.	User	*	Proxy	80	HTTP	Accept
4.	*	*	DMZ-2	*	*	Drop

* The first rule states that no mlc from any other security zone is permitted to establish a TCP connection to any internal mlc.
* Rules 2-4 assert that, other than connections from internal stations to the internal mail server (on port 25) & web proxy (on port 80), no other connections are permitted to DMZ-1, DMZ-2 or the internet.

Table: Simplified ruleset for firewall, F1.

No	from IP Addr.	from port	TO IP Addr.	TO port	protocol	Action
1	*	*	DMZ-2	*	*	Drop
2.	Int_Mail_s	*	Ext_Mail_s	25	SMTP	Accept
3.	Internet	*	"	"	"	"
4.	"	*	Web_s	80	HTTP	"
5	"	*	DNS_s	53	UDP	"
6.	*	*	DMZ-1	*	*	Drop
7.	proxy	*	Internet	80	HTTP	Accept
8.	Ext_mail_s	*	"	25	SMTP	"
9.	*	*	"	*	*	Drop.

* Rule 1 states that no Tcp connection is to be established to any mlc in DMZ-2 from any mlc in DMZ-1 or the Internet.

* Rule 2 states that the external mail server can accept connections from the internal mail server to receive incoming mail or to send outgoing mail.

* Rule 3 allows connections to the external mail server from mail servers on the internet to deposit incoming mail.
* Rule 4 & 5 permit connections from the internet to the Organization's web server & external DNS server respectively.
* Rule 6 states that no other connections may be set up to any m/c in DMZ-1 for any other purpose
* The internet proxy in DMZ-2 & the external mail server are permitted to make connections to m/cs on the Internet to access webpages & to send outgoing mail (Rules 7 & 8).
* Rule 9 confirms that no other connection from the Organization's m/cs to the internet for any other purpose is allowed.