.

1. The CSC has released Wifi solution based on Cisco Wireless Controllers for the entire academic areas/ Guest houses and Hospital. These services are accesible with SSIDs namely IITD_WIFI, IITD_Secure_GUEST and eduroam. A total of 482 Cisco Access Points (dual-band 802.11a/g/n/ac)
has been installed.

2. The CSC has also released Wifi solution based on Aruba Controllers for the common areas in all the hostels. These Wifi services are accessible using SSIDs namely IITD_WIFI, IITD_Guests/IITD_GUEST and eduroam. A total of 41 Aruba Access Points has been installed.

3. We use IEEE 802.1x (WPA2 Enterprise) based encryption for security on IITD_WIFI, IITD_Secure_GUEST and eduroam. For authentication, we use the
EAP method
EAP-TTLS
with
PAP
as the inner-tunnel method as well as the
EAP method
PEAP
with
MSCHAPv2
as the inner tunnel method . The
EAP method
EAP-TTLS with PAP as the inner tunnel method
is natively supported in Mac OS X and Linux. The
EAP method
PEAP
with
MSCHAPv2
as the inner tunnel method is natively supported on Windows platforms and is commonly available on mobile phones and other hand-held devices. Use of
PEAP/MSCHAPv2
requires registration of password with the
Microsoft Active Directory
. IITD_Guests are "Unsecured network" but uses HTTPS authentication based on captive portal technology develped in-house.

4. The RADIUS servers for EAP-TTLS and EAP-PEAP uses the IITD LDAP, Kerberos systems and /or Windows Active Directory for user authorization and authentication at the back-end. Users can connect to the Wifi network using their LDAP ids and Kerberos passwords. Upon successful authentication, clients are configured using DHCP .

5. For configuration details in your favourite laptop OS, please follow the links from the *Resources menu* on the left.

6. The locations where the Wifi access points have already been installed can be seen here .

7. Man-in-the-middle attacks and eavesdropping are easiest with wireless networks, so please make sure that you have read the Certificates section and have installed the New IITD CA certificate in your Wifi client software.

8. Please report problems, if any, to *sysadm@cc.iitd.ac.in*

9. *Please note that each user is permitted at most 8 distinct devices he can use on the IITD Wifi system in any 90 day period.*