भाग 23 / अंक 3 जुलाई 2019 त्रैमासिक पत्रिका

दूरसंचार अभियांत्रिकी केन्द्र
TELECOMMUNICATION ENGINEERING CENTRE

टी ई सी संचारिका NEWSLETTER

Telecom News: At a Glance

1. **Hon'ble Minister for Communications, Electronics & IT and Law & Justice Shri Ravi Shankar Prasad** took over the charge of communications ministry on dated 03-06-2019 at Sanchar Bhawan, New Delhi. Shri Sanjay Dhotre, Hon'ble Minister of State for Communications was also present. Hon'ble Ministers also interacted with senior officers of DoT & took a review meeting on current issues. Shri Ravi Shankar Prasad also briefed media persons about the key initiatives to be taken and priorities of the Government related to Telecom Sector at Sanchar Bhawan, New Delhi.

2. A delegation of Department of Telecommunications, Govt. of India led by Secretary (T) met H.E. Dr. Amr Talaat, Minister of Communications & IT, H. E. Khalee El Kattar, Vice Minister-Digital Transformation Automation & Admin Development and senior officials of MoCIT of Egypt to discuss the matters of mutual interests on 22-04-2019.

3. A MoU for year 2019-20 has been signed between DoT and TCIL on dated 27-05-2019 by Secretary(T) & CMD, TCIL at Sanchar Bhawan, New Delhi. TCIL, a Mini Ratna company under DoT, undertakes Projects of Telecom, IT & Civil constructions in India & abroad.

4. On the occasion of World Wi-Fi Day, a booklet on "Achieving Broadband for all under National Digital Communications Policy" was launched by Secretary(T) and Chairman, TRAI in New Delhi on dated 20-06-2019. The event was organised by ITU-APT Foundation of India.

5. 5th International Yoga Day was celebrated on dated 21-06-2019 at Sanchar Bhawan, New Delhi with participation of employees of DoT.

Digital Ledger Technology (Blockchain) – Security Aspects

1.0 Block Chain Security:

Blockchain is very complex system and comprises of distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Blockchain has the following security features:

i. Blockchain technology relies on a ledger to keep track of all financial transactions. Ordinarily, this kind of "master" ledger would be a glaring point of vulnerability. If the ledger was compromised, then it could lead to a system breakdown. For example, if someone altered a record, then they could steal a limitless amount of money. Or, if they merely read all the transactions, then they could gain access to sensitive private information. In the blockchain, the ledger is decentralized. This means no single computer or single system has control over the ledger at any point of time. It would take an incredibly sophisticated, coordinated attack on thousands of devices, simultaneously, to gain this type of access to the main ledger.

ii. Another tenet of security is the chain itself. The ledger exists as a long chain of cryptographically encrypted sequential blocks. Each chain represents another piece of the overall puzzle. Structurally, these records date back all the way to the system's launch. This means anyone who tries to alter a transaction would first have to alter all transactions leading up to that transaction, and do so accurately. This makes the hypothetical tampering process much more complicated. Also, it greatly increases the overall security of the system.

iii. Unlike present payment systems, in a block chain model there are hundreds to thousands of distinct nodes. Each node has a complete copy of the digital ledger. These can independently work to verify the transaction. If the nodes don't agree, then the transaction is cancelled. This system keeps the ledger tidy. Additionally, due to its complex mechanisms it is very difficult to commit a fraudulent transaction.

iv. The cryptographic keys along with two keys system used in block chain exchanges are very long, complex and difficult to decipher unless one has authorization to view the keys.

2.0 Block Chain Security Issues and challenges:

Blockchain has got very complex and rugged structure. In spite of this, in this technology there exists following problems and challenges w.r.t to security. Apart from double spending, which will always be possible in Bitcoin, the attack space includes a range of wallet attacks (i.e., client-side security), network attacks (such as DDoS, sybil, and eclipse) and mining attacks (such as 50%, block withholding, and bribery).

2.1. Traditional Challenges:

The use of a distributed ledger implies that data is shared between all counterparties on the network. On one side this could potentially have a negative impact on the confidentiality; while on the other, it has a positive impact on availability with many nodes participating in the Blockchain, making it more robust and resilient. Some of traditional security challenges are:

a. Key Management:

Private keys are the direct means of authorizing activities from an account, which in the event they get accessed by an adversary, will compromise any wallets or assets secured by these keys. Potentially different private keys could be used for signing and encrypting messages across the distributed ledger. An attacker who obtained encryption keys to a dataset would be able to read the underlying data. A private key is usually generated using a secure random function, meaning that reconstructing it is difficult, if not impossible. If a user loses a private key, then any asset associated with that key is lost. If a private key is stolen, the attacker will have full access to all assets controlled by that private key and once a criminal steals the key and transfer funds to another account, it cannot be undone.

b. Cryptography:

Blockchain implementations always operate on the cryptographically generated public and private keys. In case of cryptography, stringent policies and procedures are always to be followed when managing keys, including people, processes and technology. The software which is used to generate cryptographic keys should generate strong keys which could not be decrypted easily.

c. Privacy:

Privacy is an additional issue that emerges from the use of Blockchain technology. In a permissionless ledger, all counterparties are able to download the ledger, which implies that they might be able to explore the entire history of transactions, including those to which they are not members. In a permissioned ledger, exploitation of authorised agent' or smart contract capabilities could lead to severe exposure of privacy, according to the access right of the agent or smart contract authors.

2.2. The Majority Attack (51% Attacks):

With Proof of Work, the probability of mining a block depends on the work done by the miner (e.g. CPU/GPU cycles spent checking hashes). Because of this mechanism, people will want to join together in order to mining more blocks,

and become "mining pools", a place where holding most computing power. Once it holds 51% computing power, it can take control of this blockchain. This may create security issue in a chain. If someone has more than 51% computing power, then he/she can find Nonce value quicker than others, means he/she has authority to decide which block is permissible. After this attacker can:

i. Modify the transaction data, it may cause double spending attack.
ii. To stop the block verifying transaction.
iii. To stop miner mining any available block.

2.3. Distributed denial of service:

Distributed Denial of Service attacks coming out of the nature of the distributed ledger remain a concern. For example, if rogue wallets decide to push large numbers of spam transactions to the network it could create potentially a denial of service and increase the processing time, as the nodes will be checking the validity of the fraudulent transactions.

In March 2016, the Bitcoin network was slowed to a near halt. The cause was a Bitcoin wallet pushing large volumes of spam transactions with a higher than average transaction fee. This caused miners to prioritise these transactions when computing new blocks.

Within a permissioned ledger, it would be possible for nodes to agree to ignore or even block the issuer of such spam transactions. However, if an attacker is able to control a large number of clients, they might be able to severely disrupt the network by pushing large volumes of irrelevant transactions. The distributed nature of Blockchain architecture introduces the prospect that it would be difficult to shut down a malicious program.

2.4. Wallet Management:

Wallet management represents the process and technology used with which a wallet software operates with the keys assigned to it. The wallet software would need to protect the keys from being accessed without authorization, in both cases while stored, but also while in operation with the software.

Losing access to a given wallet might preclude a financial institution from authorising transactions or moving assets. It might be difficult for an entity to be aware that a malicious user has access to the wallet, because copying or stealing the keys might not leave any trace on a computer.

2.5. Eclipse Attack:

An eclipse attack is when majority of peers are malicious and they prevent the user from being connected to the network to obtain information about interested transactions. An eclipse attack is particular useful when a user has sent some bitcoins to other user in some transaction, then decides to also double spend the same bitcoins. The double spender (or user) will use the eclipse attack to prevent the other user from knowing that there is also a double spend transaction out in the open, so other user gets misled into believing that there's only the original transaction. This attacks mainly targets a single party.

2.6. Sybil Attack:

This attack affects whole network. A Sybil attack is an attack where a single adversary is controlling multiple nodes on a network. It is unknown to the network that the nodes are controlled by the same adversarial entity. For example, an adversary can spawn up multiple computers, virtual machines, and IP addresses. They can create multiple accounts with different usernames and e-mail addresses and pretend that they all exist in different countries.

2.7. Double Spending:

A client in the Bitcoin network achieves a double spend (i.e., send two conflicting transactions in rapid succession) if she is able to simultaneously spend the same set of bitcoins in two different transactions. Mainly, Double-Spending within BTC is the act of using the same bitcoins (digital money files) more than once. somehow an attacker captures 51% of the hash power of the network, double spending can happen. "Hash power" means the computational power which verifies transactions and blocks. If an attacker has this control, he/she can reverse any transaction and make a private blockchain which everyone will consider as real. But so far, no such attack has happened because controlling 51% of the network is highly cost intensive. It depends on the present difficulty of mining, the hardware price, and the electricity cost, all of which is infeasible to acquire. Blockchain network usually have the mechanism to prevent double spending. Suppose a user have 1 BTC which he tries try to spend twice. He made the 1 BTC transaction to a merchant. Now, he again signs and send the same 1 BTC on another Bitcoin address to try and trick the merchant. Both transactions go into the unconfirmed pool of transactions. But only his first transaction got confirmations and was verified by miners in the next block. His second transaction could not get enough confirmations because the miners judged it as invalid, so it was pulled from the network. But if both the transactions are taken simultaneously by the miners? When miners pull the transactions simultaneously from the pool, then whichever transaction gets the maximum number of confirmations from the network will be included in the blockchain, and the other one will be discarded. However, there is a possibility of being unfair for the merchant, as the transaction might fail in getting confirmations. That's why it is recommended for merchants

to wait for a minimum of 6 confirmations. Here, "6 confirmations" simply means that after a transaction was added to the blockchain, 6 more blocks containing several other transactions were added after it. "Confirmations" are nothing but more blocks containing more transactions being added to the blockchain. Each transaction and blocks are mathematically related to the previous one. All these confirmations and transactions are time-stamped on the blockchain, making them irreversible and impossible to tamper with. So if a merchant receives his/her minimum number of confirmations, he/she can be positive it was not a double spend by the sender.

2.8. Routing attacks:

In this attack, set of nodes are isolated from the blockchain network, delaying block propagation. In this attack, the adversary delays the delivery of a block by modifying the content of specific messages. This is possible due to the lack of encryption and of secure integrity checks of messages. In addition to these, the attacker leverages the fact that nodes send block requests to the first peer that advertised each block and wait 20 minutes for its delivery, before requesting it from another peer.

3.0 Real attack incidents:

In this section, we briefly present the existing real-world security breaches/incidents that have affected adversely to blockchain and its associated technologies;

a. One of the biggest attacks in the history of Bitcoin have targeted Mt. Gox, the largest Bitcoin exchange, in which a year's long hacking effort to get into Mt. Gox culminated in the loss of 744,408 bitcoins. However, the legitimacy of attack was not completely confirmed, but it was enough to make Mt. Gox to shut down and the value of bitcoins to slide to a three-month low.
b. **Silk Road:** In 2013, another attack called Silk Road, the world's largest online anonymous market famous for its wide collection of illicit drugs and its use of Tor and Bitcoin to protect its user's privacy, reports that it is currently being subjected to what may be the most powerful distributed denial-of-service attack against the site to date. As per initial investigations it was indicated that a vendor exploited a recently discovered vulnerability in the Bitcoin protocol known as "transaction malleability" to repeatedly withdraw coins from system until it was completely empty.
c. In August 2016, BitFinex, which is a popular cryptocurrency exchange suffered a hack due to their wallet vulnerability, and as a result around 120000 bitcoins were stolen.

4.0 Countermeasures:

In this section, the state of art security solutions that provide possible countermeasures for the array of attacks as explained above on blockchain or its different applications:

4.1. No more double spending:

The transaction propagation and mining processes in Bitcoin provide an inherently high level of protection against double spending. This is achieved by enforcing a simple rule that only unspent outputs from the previous transaction may be used in the input of a next transaction, and the order of transactions is specified by their chronological order in the blockchain which is enforced using strong cryptography techniques. This boils down to a distributed consensus algorithm and timestamping. The most effective yet simple way to prevent a double spend is to wait for a multiple numbers of confirmations before delivering goods or services to the payee. In particular, the possibility of a successful double spend decreases with increase in the number of confirmations received.

4.2. Securing wallets:

A wallet contains private keys, one for each account. These private keys are encrypted using the master key which is a random key, and it is encrypted using AES-256-CBC with a key derived from a passphrase using SHA-512 and OpenSSLs EVP BytesToKey. Private key combined with the public key generates a digital signature which is used to transact from peer-to-peer. Bitcoin already has a built-in function to increase the security of its wallets called "multi-signature", which tightens the security by employing the splitting control technique. For instance, BitGo - an online wallet which provides 2-of-3 multisignature transactions to its clients.

However, the drawback of using the multi-signature transactions is that it greatly compromises the privacy and anonymity of the user. A manual method of wallet protection was proposed which is called "cold wallet". A cold wallet is another account that holds the excess of an amount by the user. This method uses two computers (the second computer has to be disconnected from the Internet) and using the Bitcoin wallet software a new private key is generated. The excess amount is sent to this new wallet using the private key of a user. Authors of the method claim that if the computer is not connected to the Internet, the hackers will not get to know the keys, hence the wallet safety can be achieved.

4.3. Security of Networks:

In this section, we will discuss various existing countermeasures proposed for securing the core protocols and its peer-to-peer networking infrastructure functionalities Trust Zone is a technology that is used as an extension of processors and system architectures to increase their security against an array of security threats.

a. Countermeasures against DDoS Attacks:

To mitigate DDoS Attacks a Proof of Activity (PoA) Protocol was proposed which is robust against a DDoS attack that could be launched by broadcasting a large number of invalid blocks in the network. In PoA, each block header is stored with a crypt value and the user that stores the first transaction places this value. These users are called "stakeholders" in the network and they are assumed, to be honest. Any subsequent storage of transactions in this block is done if there are valid stakeholders associated with the block. Storage of crypt value is random and more transactions are stored, only if more stake users are associated with the chain. If the length of the chain is more, trustworthiness among other peers increases and more miners get attracted towards the chain. Hence, an adversary cannot place a malicious block or transaction since all the nodes in the network are governed by stakeholders.

One more possible way to mitigate DDoS attacks is by continuous monitoring of network traffic by using browsers like Tor or any user-defined web service. Applying machine-learning techniques like SVM and clustering will identify which part of the network is behaving abnormally. Hence that part can be isolated from the network until debugged. Other possible methods to protect against DDoS attacks include:

(i) configure the network in a way that malicious packets and requests from unnecessary ports will be prohibited,
(ii) implement a third party DoS protection scheme which carefully monitors the network and identify variations in the pattern.

b. Countermeasures against Eclipse Attacks:

To combat eclipse attack an additional procedure is adopted to store the IP addresses that are trustworthy. If the users are connected to other peers in the network, these peers are stored in "tried" variable. The connection of the user with the peers is dependent on the threshold of the trust factor, which varies from time to time. The users can have special intrusion detection system to check the misbehaving nodes in the network. The addresses which misbehave in the network could be banned from connections. These features can prevent the users from an eclipse attack. In particular, having a check on the incoming and outgoing connections from the node can reduce the effect of an eclipse attack.

c. Countermeasures against Sybil Attacks:

Sybil attacks are avoided in blockchain by requiring block generation ability to be proportional to computational power available through the proof-of-work mechanism. That way, an adversary is limited in how many blocks they can produce. This provides strong cryptographic guarantees of Sybil resilience.

5.0 Action items:

a. DoT studying this technology in detail and its implementation in telecom sector is being analysed. Guidelines may have to be issued for implementation of blockchain in service provider networks for identity management, database management. The usage of blockchain also provides a perfect use case for prevention of roaming fraud as it was already an issue amongst service providers. Hence service providers may have to be directed by DoT to implement blockchain in their network.

b. Blockchain has its one of main application in field of financial services in banking domains. DoT can work in collaboration with different financial institutions and work out the security threats of this technology if used in banking transactions and can help in creating more secure solution.

i. IRDBT will work and develop different use cases for applications in financial domain. DoT can work in collaboration with them for developing use cases with proper security.
ii. Meity has developed a centre of excellence of blockchain. DoT can work in collaboration with Meity to develop security guidelines for use cases developed by them.
iii. DoT is developing Central Equipment Identity registery A Central Equipment Identity Registery is a database of the IMEI numbers of blacklisted mobile handsets, while list numbers including genuine IMEI shipped by vendors/OEMs, suspect list including IMEI numbers reported in theft cases. It connects the IMEI database of all mobile network operators. It acts as a central system for all the network operators to share the black listed mobile terminals so that devices blacklisted in one network will not work on other networks even if the Subscriber Identity Module (SIM) in the device is changed. The CEIR shall be operated and maintained by DoT or any other agency designated by Government and shall be accessible to all the stakeholders including citizens to find out whether mobile device purchased by them is genuine one. TEC can work in collaboration with DoT for implementation of blockchain in CEIR and create a distributed network.

6.0 Conclusion

This technology will have a profound impact for telecom users and industries including telecom service providers. This can be major source in increasing the revenue of service providers. Hence, there is a need for identifying the roles and responsibilities of telecom users, operators and service provider with regards to security aspects in the DLT environment.

Mandatory Testing and Certification of Telecom Equipments (MTCTE)

Brief of meeting held with labs:

A meeting with designated and prospective designated labs was held at Manak Bhawan, TEC, New Delhi on 21st June 2019. Meeting was chaired by Sri A. K. Sanghi, Advisor, TEC. Meeting was widely participated by the laboratories and manufacturers of /testing and measuring instruments. Queries raised by the participants were clarified by Advisor, TEC and DDG (TC & MRA). Presentations were also made by manufacturers of testing/measuring instruments to spread knowledge / awareness among lab representative about availability of various testing/measuring instruments. The outreach programme was much appreciated by the participants.

Notification for Launch of MTCTE

Certification for following telecommunications equipment under Mandatory Testing and Certification of Telecommunications Equipment (MTCTE) has been mandatory w.e.f. 1st October 2019:

a. Telecom Equipment covered under SCS

i. **2-Wire Telecom Equipment** (Executive Telephone System, NSD/ISD Payphone, Electronic Telephone Instrument, Key Telephone Systems, 2- Line Feature Phone, Coin Box Telephone, Terminals for connecting to PSTN, CLIP Phone)
ii. **Modem**
iii. **G3 Fax Machine**
iv. **ISDN CPE**

b. Telecom Equipment covered under GCS

i. **Cordless Telephone**
ii. **PABX**

The dates for various activities for implementation of mandatory certification of telecom equipment, mentioned in para 1, are as under:

Date of opening of MTCTE Portal for registration: 05-07-2019

Date of commencement of acceptance of applications: 09-07-2019

Date of implementation for mandatory certification: 01-10-2019

Notification for relaxations/ Exemptions in MTCTE procedure

Notification for following relaxation/exemptions has been issued:

i. Test results/reports from labs accredited by ILAC signatories shall be acceptable upto 31st March'2020, as a relaxation to MTCTE procedure.
ii. Submission of test reports for few parameters shall be exempted as a relaxation to MTCTE procedure. In such cases, provisional certificate shall be issued.
iii. Provisional certificate shall be valid for the period of 2 years.
iv. Requirement of labeling on certified products shall be exempted for the initial period of six months w.e.f. 1st Oct' 2019 as a relaxation to MTCTE procedure.

Shri Anil Kumar Sanghi, Advisor & Head TEC

Anil Kumar Sanghi, an ITS officer of 1982 batch is an electronics engineer from Punjab Engineering College, Chandigarh. He has served in the telecom sector for more than 34 years in different capacities dealing with planning, development, maintenance and optimization of telecom systems which include Switching, Transmission, Internet, Data Networks, Broadband, Optical Fiber NW, Computerization etc. He has handled many important projects in Haryana, Punjab, Himachal, Rajasthan Telecom Circles and Delhi NCR. He remained associated with the E-governance projects like PAWAN in Punjab and HIMSWAN in Himachal which had a long term impact on improving connectivity across state Govt.

He was on deputation with National Disaster Management Authority (NDMA) as Joint Secretary, since Dec 2013 for 5 years and handled work related to different aspects of mitigating disasters in the area of Earthquake, Landslide, Flood, CBRN etc. and various capacity building programmes. He was also looking after the role of ICT in Disasters. In NDMA, he has conceived many projects of National importance, leveraging the technology viz National Disaster Management System (NDMS), GIS System, Mobile Radiation Detection System (MRDS), Common Alerting Protocol (CAP), Priority Call Routing, Earthquake Disaster Risk Index (EDRI) to name some of them.

He joined as Sr. DDDG, in NTIPRIT heading this organization in December 2018 and stands promoted to Advisor. On 28th May 2019, he took over the charge of Head & Advisor TEC, New Delhi an apex Telecom Institution representing interest of Department of Telecommunication with additional charge of NTIPRIT.

हिंदी कार्यशाला का आयोजन

दूरसंचार अभियांत्रिकी केंद्र, नई दिल्ली में दिनांक 18.06.2019 को एक हिंदी कार्यशाला का आयोजन किया गया। इस कार्यशाला में कुल 25 अधिकारियों/कर्मचारियों ने भाग लिया। इस कार्यशाला में अतिथि वक्ता के रूप में श्री केवल कृष्ण, सेवानिवृत्त वरिष्ठ तकनीकी निदेशक (राजभाषा विभाग) ने भाग लिया। उन्होंने कार्यालय कार्यों में हिंदी का ज्यादा से ज्यादा प्रयोग करने हेतु गूगल वॉइस टाइपिंग, गूगल–ट्रांसलेसन, मोबाइल से हिंदी में कार्य करने, क्रोम ब्राउजर का प्रयोग करके हिंदी/अंग्रेजी में डिक्टेशन देने और गूगल डॉक्स पर कार्य करने के बारे में विस्तार से उल्लेख किया एवं अभ्यास भी करवाया।

हिन्दी कार्यशाला में उपस्थित अधिकारी व कर्मचारी गण

Activities at NTIPRIT (APR-19 to JUN-19)

1. Foundation Course for ITS-2015 and P&T BWS-2017 Batch Officer Trainees:

As part of Induction Training, Officer Trainees of ITS-2015, already posted in different units of Department of Telecommunications, are called back to attend 15 weeks Foundation Course at HIPA, Gurugram. The officer trainees of P&T BWS-2017 batch also joined the Foundation Course which was inaugurated on 08.04.2019 by Director General, HIPA, Gurugram and Sh. Anil Kumar Sanghi, Advisor, NTIPRIT, Ghaziabad. The inaugural function was followed by group photograph and lunch. Sh. Rakesh Kumar Sharma, DDG (Admin.); Mrs. V Sobhana, DDG (Training); Sh. Subhash Chand, Director (Training); Sh. Manoranjan, ADG (Training) were present during the event.

Group Photograph of ITS-2015 and P&T BWS-2017 Batch with faculties of NTIPRIT and HIPA on Inaugural Day of Foundation course at HIPA, Gurugram

2. Valedictory Module of ITS-2014, P&T BWS-2015 and JTO-2016 (RL) batch:

After completion of 15 weeks Foundation course at HIPA, Gurugram, the Officers of ITS-2014 and P&T BWS-2015 batch joined back to NTIPRIT to attained 1-week valedictory module. Sh. Anil Kumar Sanghi, Advisor, NTIPRIT blessed the occasion by motivating the young officers for future endeavors.

Group Photograph of ITS-2014 and P&T BWS-2015 Batch with faculties of NTIPRIT on the occation of Valedictory Programme

After completion of 30 weeks Induction training of JTO-2016 (RL) batch, Probationers were motivated and blessed by Senior officers of NTIPRIT. Ms. V. Sobhana, DDG (Training) chaired the program on 28.06.2019.

3. Seminar on Artificial Intelligence (09-05-2019 to 10-05-2019)

Two days Seminar on Artificial Intelligence was conducted by NTIPRIT at Hotel Fortune Inn Grazia, Ghaziabad. During the course the experts from government organizations and Broad Band India Forum were invited to deliver the lectures and share the experiences. 34 Officers from various LSAs had attended the course.

Group Photograph of participated officers

4. Induction Training of the following batches of Officer Trainees of ITS/BWS probationers was conducted during the period:

ITS-2014 batch (15 officers), ITS-2015 batch (33 officers), ITS-2016 batch (34 officers), BWS-2015 batch (1 officer), BWS-2016 batch (3 officers), BWS-2017 batch (2 Officers), JTO-2016(R) Batch (2 officers).

Various training programs like technical modules, BSNL/MTNL attachment and Field Attachment for ITS/ BWS/ JTO batches, were conducted during this period as per respective training calendar.

5. In-service training courses for DoT Officers were conducted at NTIPRIT on the following topics:

i. Seminar on "Artificial Intelligence" (09-10 May, 2019) [34 Participants],

ii. Seminar on "ICT in Disaster Management" (06-07 June, 2019) [25 Participants],

iii. In-Service course on "Smart City" (18-19 June, 2019) [21 Participants],

iv. In-Service course on "Greening the Telecom for Sustainable Growth" [12 Participants]

Approvals from APR-19 to JUN-19

Sl. No.	Name of the Manufacturer/Trader & Name of Product & Model No.
A	**M/s Enjay I.T. Solutions Ltd.**
1	PABX for Network Connectivity, Enjay Synapse
B	**BPL Telecom Private Limited**
2	IP PBX with Media Gateway, AEONIX
C	**ECI Telecom India Pvt. Ltd.**
3	Interchange of Ethernet Signals Between Different Networks, Digital Multiplexer 1G, NPT-1010
4	Interchange of Ethernet Signals Between Different Networks, Digital Multiplexer 1G, NPT-1020
5	Interchange of Ethernet Signals Between Different Networks, Digital Multiplexer 1G, NPT-1021
6	Interchange of Ethernet Signals Between Different Networks, Digital Multiplexer 1G, NPT-1030
7	Interchange of Ethernet Signals Between Different Networks, Digital Multiplexer 1G, NPT-1050
8	Interchange of Digital Signals at 2 Mbit/s, 8 Mbit/s, 34 Mbit/s, 140 Mbit/s and 45 Mbit/s Ports, Digital Multiplexer, NPT-1030

Important Activities of TEC during APR 19 to JUNE 19

Brief About TEC

Telecommunication Engineering Centre (TEC) functions under Department of Telecommunications (DOT), Government of India. Its activities include:

- Issue of Generic Requirements (GR), Interface Requirements (IR), Service Requirements (SR) and Standards for Telecom Products and Services
- Field evaluation of products and Systems
- National Fundamental Plans
- Support to DOT on technology issues
- Testing & Certification of Telecom products

For the purpose of testing, four Regional Telecom Engineering Centers (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

For more information visit TEC website www.tec.gov.in

GRs/IRs/SDs/ERs issued

- GR on IDMS using CAP, GR on NTP Server
- GR on Primary Reference Clock
- SR on Time Synchronisation in IP Network
- SD on Data dictionary

DCC meeting conducted for:

- GR on HDPE duct, GR on DWC duct, GR on E-PoN
- GR on VRLA battery for UPS application
- GR on SHDSL modem,
- GR on OTDR (Mini) and OTDR Type – I

Sub DCC meeting conducted for:

- GR on Micro duct, GR on PTP Grand Master, GR on PTP slave
- Test Procedure for measurement of EMF from base station antenna

Study/white paper issued:

- 5G Transport

Other Activities

- Meetings of NWG-5, NWG-13, NWG-15 were held in TEC
- NSG-5 meeting held in TEC
- Testing for technology approval case of CDoT Wi Fi equipment carried out in CDoT Bengaluru campus
- 09 Labs were designated as CAB of TEC

Meeting/Seminar, webinar attended:

- ITU–T SG-5, SG-13 meeting was held at Geneva
- Seminar on ETSI Security at Sophia Antipolis, France
- 'Enabling 5G in India' meeting organised by TRAI in Delhi
- '5G India 2019' meeting in New Delhi
- Workshop UNESCAP sub regional at New Delhi
- ACS committee meeting at DoT, Sanchar bhawan, Delhi
- 3rd Global meeting on 'AI for Good-Global summit' held in Geneva by ITU-T
- Lakshdweep submarine cable committee by USOF in DoT HQ
- Two days seminar on 'ICT in Disaster Management' at NTIPRIT, Ghaziabad
- Meeting of DoT committee on BRICS for establishing a branch of BRICS Institute of Future Networks in India.

Presentation/Training/Seminar/Meetings workshop webinar

- A presentation on Open Source Intelligence Tools was given by M/s Verient.
- A presentation on implementation of DNS in its network is given by M/s Tata Communication Ltd.

Contributions submitted to ITU-T/R/D

- 03 contributions were submitted to SG-5 of ITU-R
- 01 contribution related to unified portal for EMF exposure assessment was submitted to SG-5 of ITU-T
- 03 contributions as below were submitted to SG-15 of ITU-T;
  - i. Contribution on draft new recommendation ITU-T. L.fdb "Requirement for passive optical nodes: Fibre distribution Box"-Proposal to add Appendix II as Indian Experience
  - ii. Contribution on draft new recommendation ITU-T. L.tifm "Telecommunication infrastructure facilities management"-Proposal for revision of text
  - iii. Contribution as a new proposal for draft Rec. L.font "Requirement for a combined Fibre Optical Network Terminal Box: Font

Suggestions/feedback are welcomed, if any for further improvement.

टी ई सी संचारिका : दूरसंचार अभियांत्रिकी केन्द्र
जुलाई 2019 : खुर्शीद लाल भवन
भाग 23 : जनपथ
अंक 3 : नई दिल्ली–110001

Editor : Ram Lal Bharti, DDG (NGS) Phone : 23329354 Fax : 23318724 E-mail : ddgs.tec@gov.in

Printed at : Yugantar Prakashan Pvt. Ltd., New Delhi; M:9811349619