INTERNET DATA CENTRE

GENERIC REQUIREMENTS

No. TEC/GR/SA/IDC-001/02MAR2010

(Superseeds GR. No. GR/IDC-01/01 OCT2001)

TELECOMMUNICATION ENGINEERING CENTRE
KHURSHID LAL BHAWAN, JANPATH
NEW DELHI – 110 001
INDIA

TELECOMMUNICATION ENGINEERING CENTRE
(DEPARTMENT OF TELECOMMUNICATIONS)

Generic Requirements for “IDC” TEC/GR/SA/IDC-001/02 MAR2010”

History Sheet

Sl No.	Number/Name	Description
1	GR/IDC-01/01 OCT 2001. GR for IDC	First edition of GR for the Internet Data Centre
2	TEC/GR/SA/IDC-001/02 MAR2010	Second issue after review

INDEX

1. Introduction

1.1 This document specifies the generic requirements for defining technical requirements of a Internet Data Center (IDC). The IDC is a secure physical facility with round the clock customer support, backup power, controlled environment, hardware and software infrastructure. It shall house the various hardware and software components relating to the hosting services. The data center should be accessible to different ISPs and other Data Centres. The IDC through appropriate infrastructure shall ensure host, content, and application availability as well as guaranteed security and network performance.

1.2 **Scope:** This document defines the generic physical and logical infrastructure required for providing the Internet Data Center.

2 Description

2.0 This clause on Internet Data Center (IDC) contains the technical requirement of a secure infrastructure with round the clock operational support for services like Application Hosting, Web Hosting, e-commerce etc. This clause provides the requirements of state-of-the-art IDC that allows provisioning of intelligent Internet services in a cost-effective and reliable manner.

2.1 Internet data centre(IDC) shall be required to be maintained round the clock with a disaster recovery node where critical components are replicated so that in the normal course, they can work in a load sharing and redundant mode. It shall house all the hardware and software, including servers, routers, and switches for network connections, load balancing software/hardware to guarantee performance and ensure service level agreements(SLAs);security through dedicated or software firewalls; backup systems, and other equipment.IDC shall also house a network operations center(NOC) which shall be typically server management and configuration system. The data centre also shall be equipped with fire suppression, uninterrupted power supply(UPS), and disaster recovery systems.

2.2 Service providers with access and backbone infrastructure will be able to offer Web hosting services with cost advantages as Web hosting requires a large supply of bandwidth. The connectivity diagram for the data centers to the IP network is shown in figure -1.

3 Functional Requirements

3.0 Technical Requirements of Internet Data Centre

3.0.1 **T**he IDC should support advanced networking features including content networking capabilities, which should enable the network to interact with the servers to deliver content and applications in a scalable and reliable fashion. The important requirements of content networking shall be:.

a) Localizer and global content distribution, dynamic content delivery, and effective local and geographical server load balancing.
b) Capability of the network to identify and process packets based on application type and user type.
c) High security against physical as well as network intrusion.
d) Caching and load-balancing functions to achieve the best performance and response time.
e) Local Peering to Internet Exchange Point to allow the clients to get to IDC site faster while reducing the cost of the bandwidth.
f) It should be capable of supporting the Fiber Channel over Ethernet Standard (FCoE) for linkages to Storage Area networks

3.0.2 The Data center shall satisfies the following requirements:

a) Multiple physical locations and load balancing across these locations.
b) Multiple Wide Area Links from a single locations to different destination.
c) Load balancing on TCP ports.
d) Policy-based flow setup with distributed network processors that support wire-speed flow forwarding
e) Real time intrusion detection thorough passive promiscuous monitoring of network segments, routers, firewalls or switch ports. This should have active TCP resets and Access Control lists (ACL) modifications to respond to attacks.
f) LAN switch with full layer 3 switching capability.
g) QoS supported on the switch(Weighted Fair Queing WFQ, Weighted Random Early Detection WRED etc).
h) Security based on Stateful failover to guarantee availability.
i) Prevention of Denial of Service Attacks.
j) Support for Web cache protocol and reverse proxy.

3.1 Functional requirements: The architecture and network layout for the Data Center should be as given in figure - 2 It shall consist of the following components:

3.1.1 Content Provisioning System: This includes the equipments where the content resides. It shall consist of server farms with applications hosted by the service providers. The servers in IDC shall have capability to handle distributed Internet traffic effectively across the Local Area Network ensuring the fastest response, while decreasing the potential for failures.

3.1.2 Access Provisioning System :The Access Provisioning System shall consists of LAN switches to interconnect to the servers over Ethernet. The LAN switches shall comply with the requirements specified in TEC GR No.

GR/LSW-01/03.SEP.2007 for sub-category 1-C of LAN switches with latest amendments

3.1.3 **Distribution Systems**: The distribution Systems provides content based intelligent network services through Web switches, Traffic Directors, Load Balancers and Web Cache Devices. The main function of the Distribution System shall be to seamlessly route specific web user requests based on requested content to the best server among a multiplicity of servers located in the same or different locations. Web switches shall connect to the core switches and the access switches. The details are available at clause 2.2 of this GR.

3.1.4 **Core Connectivity System:** This System is responsible for the aggregation of the traffic. The user data is handed over to the distribution layer where content networking and other intelligent processing is applied on the traffic, This system also connects to the border routers at the periphery of the IDC network. The details are available at clause 2.3 of this GR.

3.1.5 **Border Connectivity System :** The border connectivity system shall consists of high-end routers to manage the traffic in and out of the IDC. It shall comply with the requirements specified in TEC GR No.TEC/GR/SA/TCP-001/03 MAR 2009 with latest amendments for sub category 1-A(Gateway Router).

3.1.6 **Security System :** The Security system of the Internet Data System shall be as per the Information Technology(IT)Security Guidelines contained in the Information Technology (Certifying Authority) Rules, 2000 with latest amendments.

3.2 **Distribution System :** The Distribution Systems are responsible for efficient routing of web requests based on the content type requested to the best suited server among the server farms. This is the heart of the IDC and provides intelligent services based on the content requested, traffic type etc. The Distribution Systems shall consists of the following components:

3.2.1 **Web Switch :** The web switch shall comply with following requirements:

3.2.1.1 **Performance :** The web switch shall have a high-performance, modular chassis based on distributed processing architecture.

3.2.1.2 The web switch shall support redundant power supplies, control modules and switching fabric.

3.2.1.3 It shall support the following performance specifications *in a single chassis*:

(a) Switching capacity of at least 100 Gbps
(b) Memory of 2GB.
(c) The layer2 and layer 3 performance shall be wired (copper/fiber) speed with a support of at least Packet forwarding rate of 100 million packets per second
(d) Support for at least 1 million simultaneous HTTP sessions
(e) Support for at least 1 million simultaneous TCP sessions
(f) HTTP flow rate of at least 100,000/second

3.2.1.4 It shall support the following minimum Interface requirements in a single chassis:

Sl. No.	Interface Type	No. of Ports
1	1000 Base-TX, RJ45 Interface	16
2	1000Base-SX Full duplex-	16
3	10 Gigabit Full Duplex	2

3.2.1.5 **Layer 5 capabilities**:: The web switch is capable of making intelligent switching and forwarding decisions based on Layers 2,3,4 and 5 of the TCP/IP protocol stack. The web switch shall possesses the following capabilities:

(a) Intelligently process traffic based on IP, TCP, URL, cookies and SSL session ID information.

(b) **Delayed Binding** - ability to delay the connection of user to the site and server until receipt of HTTP request from the user (and not at the initial connection) which contains the full URL and cookie information.

(c) **URL and Cookie based switching:** The ability to select the best site and server for each user based on actual content being requested. The decision shall be based on full URL and cookie in the HTTP header. It shall be possible to apply policies like access control, server response times, and application availability and priority levels to the switching process.

(d) Ability to read any cookie header, regardless of where the cookie resides in the packet.

(e) Ability to read up to 1000 bytes of URL and cookie information in the HTTP request header to enable full parsing of that information for forwarding decisions.

(f) **Persistent or “sticky” connections:** Ability to map the user to the same server for each request until the transaction is completed. The sticky connection support shall be based on the following parameters – IP address, TCP port, SSL session ID and embedded cookie in the HTTP header.

3.2.1.6 Load Balancer: The Load Balancer functionality may be a part of the Web switch. However, for better performance, a dedicated Load Balancer separate from the web switch is recommended. The web switch shall be capable of supporting intelligent load balancing on the same chassis without any external device. It supports the following features:

(a) Support for following load balancing algorithms - Round Robin, Weighted Round Robin, Least Connections, Server Load

(b) Network Address Translation (NAT) peering to direct users to best site and server. The web switch shall communicate with other peer web switches in the country to maintain and share real time information on the status of servers in all the IDCs.

(c) **Flash crowd and hot content replication:** The web switch shall be capable of dynamically tracking content requests to identify sudden increases in specific content requests and replicate these “hot” content in additional servers or cache in local or distributed IDCs to balance the load and maintain service levels.

(d). Automatic content replication based on time-of-day or content modification

3.2.1.6.1

3.2.1.6.1(a) Local Director: Local Director shall provide load balancing of TCP/UDP services. It automatically directs requests to the best available local server within the data center and automatically directs traffic away from unavailable application servers.

Local Director shall make decisions based on server feedback using DFP, Web probing capabilities through the internal statistical algorithms.

3.2.1.6.1(b) Virtualization – The web switch and the Load Balancer shall be capable of supporting the feature of virtualization.

3.2.1.6.2 Distributed Director: Distributed Director should be a Content Flow-based geographical load distribution device that can select specific data centers to enable global scalability of Internet and intranet services. Distributed Director shall provide transparent access to the closest available data center relative to the client as determined by client-to-server topological proximity and/or link latency. It maps a single DNS hostname to the closest data center relative to the client, eliminating the need for end-users to choose from a list of URL hostnames to find the best server. It automatically shall directs traffic away from unavailable servers or data centers. The Distributed Director shall support both “local routing” and “Global routing”. Both functionalities can exist on the same device . However, for better performance, they should be on separate devices. Distributed Director shall support high availability and failover.

3.2.1.7 Caching: The caching feature should be available either as a part of web switch or as a separate device. However, for better performance, caching device should be separate from the web switch.

Cache feature built into the web switch - The web switch shall support content distribution and delivery with external cache devices. It shall be possible to configure the web switch with content policies to make intelligent caching decisions. The following capabilities shall be supported:

(a) Proxy, Transparent and Reverse Proxy Cache configurations

(b) Cache bypass for non-cacheable content. The web switch shall be capable of ensuring that requests for dynamic content like stock quotes are offloaded from the cache. Bypass shall be based on: Source IP address, Destination IP address, TCP Port, Host Tag, URL, file type

(c) Bypass of reverse proxy cache for dynamic, non-cacheable content.

(d) Cache distribution based on Source IP address hash, Destination IP address hash, Domain Name (Host Tag), URL (Content affinity), Cache Load

3.2.1.8 Management: The web switch shall supports the following management capabilities

(a) Provide statistics and accounting on a per-flow and transaction basis.

(b) Ability to track traffic on a per domain-name basis and per URL basis

(c) Support for SNMP ver2 and RMON

(d) Management port with command line interface support

For increased performance of the web switch, the functionalities at (a) and (b) above can be provided separately in dedicated devices not part of the web switch.

3.2.2 Separate Cache Device: The distribution system shall also consist of high performance dedicated Caching equipment. The function of the cache device is to accelerate content delivery, optimize WAN bandwidth utilization, and control access to content in the IDC. The required features for the cache device is given below:

3.2.2.1 It shall be a dedicated high performance hardware device. The cache device shall be able to operate as a single unit and as part of a cache farm through clustering

3.2.2.2 Performance: The cache device shall support the following specifications

(a) At least 300 GB of storage capacity. .

(b) Redundant power supplies.
(c) Two 100BaseTX Ethernet ports
(d) At least 2000 GB of storage capacity as a cluster
(e) Random Access Memory capacity of 32 GB or more
(f) At least 800 concurrent TCP sessions per device and at least 25,000 TCP sessions in a cluster.
(g) The cache device shall be able to operate in a fail-safe mode in a cluster so that if the entire cache farm fails, the operation of the IDC is unaffected.
(h) The cache device shall be fault tolerant in a cluster mode to ensure that individual failures of cache devices do not affect the operations of the cache cluster.
(i) Multi-homing support to connect to two routers simultaneously.
(j) Configurable bypass capabilities :
(k) Proxy mode should be supported by the caching device. The Reverse Proxy mode should be available either in the caching device or as a separate device if not available in the caching device.
    i. Dynamic client bypass to enable users to directly connect to server.
    ii. Failure bypass to enable cache device to be bypassed in case of failure of the device..
    iii. Static bypass for administratively configuring bypass for specific addresses.

3.2.2.3 **Manageability:** The cache device shall support the following features:
(a) Generate the following statistics - total number of requests, total bytes transferred most commonly requested URLs, most common IP addresses making requests, performance during peak periods, cache hit rates.
(b) SNMP and cache MIB support
(c) Telnet, FTP and syslog
(d) Web based GUI

3.3 **Core Connectivity System :** At the core layer the aggregation of the traffic occurs and user data is handed over to the distribution layer where content networking and other intelligent processing is applied on the traffic. It shall also connect to the border routers at the periphery of the IDC network.

3.3.1 **T**he core system shall consists of high performance LAN switches to efficiently handle the high volumes of IDC traffic. The Core LAN switch comply with the requirements specified in TEC GR No. GR/LSW-01/03 SEP 2007 for sub-category 1-A of LAN switches.

3.3.2 The core layer shall offer the following wire-speed IP services :

a) Quality of service
b) Security
c) Scalable routing protocols
d) Multi Protocol Label Switching (MPLS) based Virtual Private Networks (VPN).

3.4 Service Model for Web hosting: IDC shall supports following various broad service models for the Web hosting:
a) Simple Hosting
b) Collocation Hosting
c) Managed Hosting
d) Full Service Hosting

3.4.1 Simple Hosting: Simple Hosting consists of the basic Web Hosting sites where little or no application integration shall be required. It shall have at least web or E-Commerce skill capability. The service description for simple web hosting shall consist of :
a) Shared or dedicated servers
b) Box and systems monitoring

3.4.2 Collocation Hosting: This shall consists of more skill for web or E-commerce hosting, so that it can effectively become an Intranet or Extranet business site. The service description for collocation hosting shall consists of::
a) Racks, cages, physical security, redundant power
b) Bandwidth, network redundancy, multiple peering
c) Box monitoring, remote administration tools

3.4.3 Managed Hosting: This shall consist of extensive managed web sites, which are meant for global operation. The service description shall consist of:
a) All collocation services
b) Custom server management configuration
c) Back-end network integration
d) Systems and apps monitoring

3.4.4 Full Service Hosting: The full service-hosting model shall consist of facility to handle complex legacy equipment. It consists of :
a) All managed services
b) System integration
c) Consulting design, configuration, management

3.5 Enhanced Services : IDC shall support the following enhanced services for the Co-Location customers, Managed Solutions customers and Full Service solution customers to opt for additional Enhanced Services tailored to meet their demands:

a) Storage Area Networking (SAN) for a localized integrated storage of data. Storage Area Networking should support “Virtualization in SAN”, “Inter-VSAN Routing” and Fiber Channel over IP (FCIP) Technology.

b) Tape Back-up Services: Protection against data loss due to accidents, hardware failures or disaster as well as fast and accurate data recovery services. It shall support:
   - i. Prompt recovery options in the event of downtime
   - ii. Daily, weekly, and monthly reporting of backup and restore processes available via a password protected Web site
   - iii. Enhanced capabilities for backing up large volumes of data
   - iv. Scalable storage solutions to match your growth requirements
   - v. Special backup event setup
   - vi. Tape Libraries should be shareable across VSANs.

c) Customer **Escalation:** The IDC administrators as a policy should be able to notify customers of any critical conditions that occur during the backup and restore process.

d) Disaster Recovery Services for handling failures easily. High Bandwidth connectivity between IDCs to enable mirroring the site on a transaction to transaction basis shall be supported.

e) Enhanced Monitoring Services to keep a round the clock close watch over the Web sites, systematically monitoring hardware failures, software processes, URLs, Ports, Network Connectivity shall be supported.

f) Managed Firewalls with state-of-the-art security management & firewall technology to ensure the IDC highest level of protection shall be supported.

g) Load Balancing Services - Both Server and global load balancing solutions shall be available.

h) High Availability and replication Services to ensure no failures for server operation.

i) Billing: IDC shall consist of a billing solution, which would be able to give customizable solution based on the following parameters:
   - i. Per flow Data Export consisting of a Collection Engine and External Billing Interface
   - ii. Switch MIB statistics with Virtual Web Hosting (# Hits, # Hit missed, # Bytes, etc)
   - iii. Customizable Billing Solution

j) Managed Monitoring Service : IDC shall have provision to manage and monitor the network and URL, analyze the trends and build strategies based on known system utilization. Using this the following managed monitoring service to the IDC with next generation monitoring and reporting tools for proactive systems management shall be supported :
   - i. Bandwidth reporting
   - ii. Historical performance trend reporting

iii. URL monitoring and events log

iv. System administration

k) The typical examples of different packages that shall be provided to different customers based on their requirements shall be supported and shallbe as given below:

i. Managed Monitoring Services for Entry Level : The system is capable for getting tailored to offer a general, integrated location for viewing real-time network and system information, status updates on URL and historical bandwidth reports.

ii. Managed Monitoring Service for more than Entry Level:: The system shall be capable to offer server monitoring with the ability to monitor their servers in real-time. IDC shall be also able to define critical thresholds for servers and have the System alert the customers when the thresholds are reached.

iii. Managed Monitoring Service for the highest level : IDC shall have facility to meet the high-level needs for real-time systems monitoring and management. It shall include problem resolution for say, up to four events per month, historical graphs on server performance and past trends, as well as automated process restarts when required. In addition, this highest end service shall provide monitoring for extra URLs and hourly reports on bandwidth usage.

3.6 Engineering Requirements.

a) The equipment shall be compact, composite construction and lightweight. The actual dimensions and weight of the equipment shall be furnished by the manufacturers.

b) All connectors shall be reliable, low loss and standard type so as to ensure failure free operations over long operations.

c) All LAN cabling shall be of Gigabit Ethernet ready as per TEC GR No. GR/SLC-01/02 SEP 2005 and as amended from time to time.

d) The equipment shall have adequate cooling arrangements.

e) Each sub-assembly shall be clearly marked with schematic reference to show its function, so that it is identifiable from the layout diagram in the handbook.

f) Each terminal block and individual tags shall be numbered suitably with clear identification code and shall correspond to the associated wiring drawings.

g) All controls, switches, indicators etc. shall be clearly marked to show their circuit diagrams and functions.

4. Interconnectivity & Inter operability

4.0 Web Switch :

Protocol support: The Web switch shall support the following protocols:

(a) TCP, FTP, FTP (Dynamic), UDP, HTTP, secured HTTP (SHTTP), SMTP, NNTP, DNS, OSPF,POP3,IMAP<RADIUS..

(b) The Web switch shall support WAP traffic and provide load balancing fo r the same.

(c) MAC Address Translation, Inbound NAT, Outbound NAT

(d) ICMP Ping, TCP Connection Observation (TCO), TCP Connection Verification (TCV)

(e) HTTP GET, HTTP POST, URL,FTP,NNTP,SMTP POP3,IMAP, DNS, RADIUS, WAP, HTTP-s and custom scripts for content verification

4.1 Cache Device :

Protocol support: The following protocols shall be supported for the cache device

(a) Web Cache Communication Protocol (WCCP) ver 2; Internet Cache protocol (ICP) as per RFC 2186

(a) HTTP 1.0, 1.1

(b) RADIUS

5. Quality Requirements

5.1 QUALITATIVE REQUIREMENTS (QR) The system shall meet the following qualitative requirements:

a. The supplier / Manufacturer shall manufacture with international quality standards ISO 9002 for which the manufacturer shall be duly accredited. The quality plan describing the quality assurance system followed by the manufacturer shall conform to the guidelines given by CGM QA from time to time and shall be submitted.

b. The MTBF (Mean Time Between Failure) and MTTR (Mean Time To Restore) predicted. and observed values shall be furnished along with the calculations by the manufacturer

c. The equipment shall meet the Electromagnetic Compatibility (EMC) requirements as specified in Annexure 1 of TEC GR No. G / PRI-01.

6. EMI/EMC Requirements

6.1 Electromagnetic Interference

The equipment shall conform to the following EMC requirements for Class A:

General Electromagnetic Compatibility (EMC) Requirements: - The equipment shall conform to the EMC requirements as per the following standards and limits indicated therein. A test certificate and test report shall be furnished from a test agency.

a) Conducted and radiated emission *(applicable to telecom equipment)*:

Name of EMC Standard: "CISPR 22 (2005) with amendment 1 (2005) & amendment 2 (2006) – Limits and methods of measurement of radio disturbance characteristics of Information Technology Equipment".

Limits:-

To comply with Class A or B (to be mentioned in the GR / IR as per the specific requirement) of CISPR 22 (2005) with amendment 1 (2005) & amendment 2 (2006).

ii) The values of limits shall be as per TEC Standard No. TEC/EMI/TEL-001/01/FEB-09**.**

OR

Conducted and radiated emission (applicable to instruments such as power meter, frequency counter etc.):

Name of EMC Standard: "CISPR 11 {2004}- Industrial, scientific and medical (ISM) radio- frequency equipment-Electromagnetic disturbance characteristics- Limits and methods of measurement"

Limits :-

i) To comply with the category of Group 1 of Class A of CISPR 11 {2004}

ii) The values of limits shall be as per clause No. 8.5.2 of TEC Standard No. TEC/EMI/TEL-001/01/FEB-09**.**

b) Immunity to Electrostatic discharge:

Name of EMC Standard: IEC 61000-4-2 {2001) "Testing and measurement techniques of Electrostatic discharge immunity test"**.**

Limits: -

i) Contact discharge level 2 {± 4 kV} or higher voltage;

ii) Air discharge level 3 {± 8 kV} or higher voltage;

c) Immunity to radiated RF:

Name of EMC Standard: IEC 61000-4-3 (2006) "Testing and measurement techniques-Radiated RF Electromagnetic Field Immunity test"

Limits:-

For Telecom Equipment and Telecom Terminal Equipment with Voice interface (s)

i) Under Test level 2 {Test field strength of 3 V/m} for general purposes in frequency range 80 MHz to 1000 MHz and

ii) Under test level 3 (10 V/m) for protection against digital radio telephones and other RF devices in frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz.

For Telecom Terminal Equipment without Voice interface (s)
Under Test level 2 {Test field strength of 3 V/m} for general purposes in frequency range 80 MHz to 1000 MHz and for protection against digital radio telephones and other RF devices in frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz.

d) Immunity to fast transients (burst):
Name of EMC Standard: IEC 61000- 4- 4 {2004) "Testing and measurement techniques of electrical fast transients/burst immunity test"

Limits:-

Test Level 2 i.e. a) 1 kV for AC/DC power lines; b) 0. 5 kV for signal / control / data / telecom lines;

e) Immunity to surges:
Name of EMC Standard: IEC 61000-4-5 (2005) “Testing & Measurement techniques for Surge immunity test"
Limits:-
i) For mains power input ports : (a)1.0 kV peak open circuit voltage for line to ground coupling (b) 0.5 kV peak open circuit voltage for line to line coupling

ii) For telecom ports : (a) 0.5 kV peak open circuit voltage for line to ground (b) 0.5 KV peak open circuit voltage for line to line coupling.

f) Immunity to conducted disturbance induced by Radio frequency fields:
Name of EMC Standard: IEC 61000-4-6 (2003) with amendment 1 (2004) & amd. 2 (2006) "Testing & measurement techniques-Immunity to conducted disturbances induced by radio- frequency fields "

Limits:-
Under the test level 2 {3 V r.m.s.}in the frequency range 150 kHz-80 MHz for AC / DC lines and Signal /Control/telecom lines.

g) Immunity to voltage dips & short interruptions (applicable to only ac mains power input ports, if any):
Name of EMC Standard: IEC 61000-4-11 (2004) “Testing & measurement techniques- voltage dips, short interruptions and voltage variations immunity tests”
Limits:-
i) a voltage dip corresponding to a reduction of the supply voltage of 30% for 500ms(i.e. 70 % supply voltage for 500 ms)
ii) a voltage dip corresponding to a reduction of the supply voltage of 60% for 200ms; (i.e. 40% supply voltage for 200ms) and
iii) a voltage interruption corresponding to a reduction of supply voltage of > 95% for 5s.

Note 1 : Classification of the equipment:

Class B: Class B is a category of apparatus which satisfies the class B disturbance
limits. Class B is intended primarily for use in the domestic environment

and may include:

- Equipment with no fixed place of use; for example, portable equipment powered by built in batteries;
- Telecommunication terminal equipment powered by the telecommunication networks
- Personal computers and auxiliary connected equipment.

Please note that the domestic environment is an environment where the use of broadcast radio and television receivers may be expected within a distance of 10 m of the apparatus connected.

Class A: Class A is a category of all other equipment, which satisfies the class A limits but not the class B limits.

Note 2: The test agency for EMC tests shall be an accredited agency and details of accreditation shall be submitted.

Alternatively EMC test report from a non-accredited test lab, which is audited by an accredited lab / accrediting authority for the availability of all the essential facilities (test equipment, test chamber, calibrations in order, test instructions, skilled personnel etc.), required for performing the tests according to the EMC test methods audited, may be acceptable.

However, such accredited lab / accrediting authority should take responsibility of the test results of the “non accredited lab” along with indication of period of such delegation and the submitted test report should be of such valid period of delegation. The audit report, mentioning above facts, should be provided along with EMC test report.

Note 3 :- For checking compliance with the above EMC requirements, the method of measurements shall be in accordance with TEC Standard No. TEC/EMI/TEL-001/01/FEB-09 and the references mentioned therein unless otherwise specified specifically. Alternatively, corresponding relevant Euro Norms of the above IEC/CISPR standards are also acceptable subject to the condition that frequency range and test level are met as per above mentioned sub clauses (a) to (g) and TEC Standard No. TEC/EMI/TEL-001/01/FEB-09. The details of IEC/CISPR and their corresponding Euro Norms are as follows:

IEC/CISPR	Euro Norm
CISPR 11	EN 55011
CISPR 22	EN 55022

EC 61000-4-2	EN 61000-4-2
IEC 61000-4-3	EN 61000-4-3
IEC 61000-4-4	EN 61000-4-4
IEC 61000-4-5	EN 61000-4-5
IEC 61000-4-6	EN 61000-4-6
IEC 61000-4-11	EN 61000-4-11

7. Safety Requirements:

i. The operating personnel shall be protected against shock hazards as per **IS 8437 (1993)** – Guide on the effects of current passing through the human body (equivalent to IEC publications 479-1 (1984). The manufacturer / supplier shall submit a certificate in respect of compliance to these requirements.

ii. The equipment shall conform to **IS 13252 (1992)** – Safety of Information Technology equipment including electrical business equipment (equivalent to IEC publication 95 (1986) and IEC 215 (1987) Safety requirements of Radio transmitting equipments (for Radio equipments only). The manufacturer/ supplier shall submit a certificate in respect of compliance to these requirements.

8. Security Requirements

8.0 Security Administration and Management:
The IDC shall have Security Administration and management function for administering security policy and managing security related information. These features shall be provided by NMS/EMS, if not indicated otherwise. It shall as per clause 3.5.3 of TEC standard on NMS: SD/NMS-01/01.

8.1 **Security requirements:** The firewall functionality shall be provided either in the web switch or separately through a dedicated device. Separate functionality through dedicated device is recommended for better performance of web switch. The firewall shall confirm to TEC GR No. GR/FWS-01/02 SEP 06 and as amended from time to time.

9. Other Mandatory Requirements

9.1 **Operational Requirement (OR):** The system shall meet the following maintenance & operational requirements:

a) The equipment shall be designed for continuous operation.

b) The equipment shall be able to perform satisfactorily without any degradation at an altitude upto 3000 meters above mean sea level.

c) Wherever the visual indications are provided, green colour for healthy and red colour unhealthy conditions shall be provided. Some other colour may be used for non-urgent alarms.

d) The design of the equipment shall not allow plugging of a module in the wrong slot or upside down.

e) The removal or addition of any cards shall not disrupt traffic on other cards.

f) All mission critical modules shall be identified and provided in full redundant configuration for high reliability.

g) A single point failure on the equipment shall not result in network or network management system downtime.

h) Special tools required for wiring shall be provided along with the equipment.

i) In the event of a bug found in the software, the manufacturer shall provide patches and firmware replacement if involved, free of cost. Compatibility of the existing hardware shall be maintained with future software/firmware.

j) In the event of a full system failure, a trace area shall be maintained in non-volatile memory for analysis and problem resolution.

k) Necessary alarms (indicators) for indication of faults at various levels of hardware shall be provided on the individual modules.

l) A power down condition shall not cause loss of connection configuration data storage.

m) Live Insertion and hot swap of modules shall be possible to ensure maximum network availability and easy maintainability.

n) The Hardware and software components shall not pose any problems in the normal functioning of all network elements wherever interfacing with BSNL/MTNL network for voice, data and transmission systems, as the case may be.

9.2 Other Requirements:

a) The system hardware / software shall not pose any problem, due to changes in date and time caused by events such as changeover of millennium / century, leap year etc., in the normal functioning of the system.

b) Wherever, the standardized documents like ITU-T, IETF, QA and TEC documents are referred, the latest issue and number with the amendments shall be applicable.

c) **Power Supply:** The equipment power supply requirements are given for each of the category. In addition, it shall meet the following requirements:

I) The equipment shall be able to function over the range specified in the respective chapters, without any degradation in performance.

II) The equipment shall be protected in case of voltage variation beyond the range specified and also against input reverse polarity.

III) The derived DC voltages shall have protection against short circuit and overload.

9.3 DOCUMENTATION and INSTALLATION

9.3.1 Documentation

This clause describes the general requirements for documentation to be provided.

All technical documents shall be in English language both in CD-ROM and in hard copy.

9.3.1.1 The documents shall comprise of :

System description documents
Installation, Operation and Maintenance documents
Training documents
Repair manual.

9.3.1.1.1 System description documents : The following system description documents shall be supplied along with the system.

a) Over-all system specification and description of hardware and software.

b) Equipment layout drawings.
c) Cabling and wiring diagrams.
d) Schematic drawings of all circuits in the system with timing diagrams wherever necessary.
e) Detailed specification and description of all Input / Output devices
f) Adjustment procedures, if there are any field adjustable units.
g) Spare parts catalogue - including information on individual component values, tolerances, etc. enabling procurement from alternative sources.
h) Detailed description of software describing the principles, functions, and interactions with hardware, structure of the program and data.
i) Detailed description of each individual software package indicating its functions and its linkage with the other packages, hardware, and data.
j) Program and data listings.
k) Graphical description of the system. In addition to the narrative description a functional description of the system using the functional Specification.

9.3.1.1.2: System operation documents : The following system operation documents shall be available.

a) Installation manual and testing procedures.
b) Precaution for Installation Operation and Maintenance.
c) Operation and Maintenance manual of the system.
d) Safety measures to be observed in handling the equipment
e) Man-machine language manual.

f) Fault location and trouble shooting instructions including fault dictionary.

g) Test jigs and fixtures required and procedures for routine maintenance, preventive maintenance and unit / card / sub-assembly replacement.

h) Emergency action procedures and alarm dictionary.

9.3.1.1.3: Training Documents:

a) Training manuals and documents necessary for organizing training in installation, operation and maintenance and repair of the system shall be made available.

b) Any provisional document, if supplied, shall be clearly indicated. The updates of all provisional documents shall be provided immediately following the issue of such updates.

c) The structure and scope of each document shall be clearly described.

d) The documents shall be well structured with detailed cross-referencing and indexing enabling easy identification of necessary information.

e) All diagrams, illustrations and tables shall be consistent with the relevant text.

9.3.1.1,4 Repair Manual:

a) List of replaceable parts used

b) Detailed ordering information for all the replaceable parts

c) Procedure for trouble shooting and sub-assembly replacement

d) Test fixtures and accessories for repair

e) Systematic trouble shooting charts (fault tree) for all the probable faults with their remedial actions.

9.3.2 Installation :

a) All necessary interfaces, connectors, connecting cables and accessories required for satisfactory installation and convenient operations shall be supplied. Type of connectors, adopters to be used shall be in conformity with the interfaces defined in this GR.

b) It shall be ensured that all testers, tools and support required for carrying out the stage by stage testing of the equipment before final commissioning of the network shall be supplied along with the equipment.

c) All installation materials, consumables and spare parts to be supplied.

d) All literature and instructions required for installation of the equipment, testing and bringing it to service shall be made available in English language.

e) For the installations to be carried out by the supplier, the time frames shall be furnished by the supplier including the important milestones of the installation process well before commencing the installations.

f) The equipment shall have:
   - i) Proper earthing arrangement,
   - ii) Protection against short circuit / open circuit
   - iii) Protection against accidental operations for all switches / controls provided in the front panel.
   - iv) Protection against entry of dust, insects and lizards.

Abbreviations

ACL	Access Control List
ASP	Application Service Provider
EMC	Electro Magnetic Compatibility
FTP	File Transfer Protocol
HTTP	Hiper Text Transfer Protocol
IDC	Internet Data Centre
ISP	Internet Service Provider
LAN	Local Area Network
MTBF	Mean Time Between Failure
MTTR	Mean Time To Restore
NAT	Network Address Translation
NOC	Network Operation Centre
QA	Quality Assurance
SLA	Service Level Agreement
TCP	Transmission Control Protocol
TEC	Telecom Engineering Centre
TFTP	Trivial File Transfer Protocol
URL	Universal Resource Locator
UDP	User Datagram Protocol
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Detection
WAN	Wide Area Network
WCCP	Web Cache Communication Protocol
WWW	World Wide Web

Data Center Network Architecture Nationwide

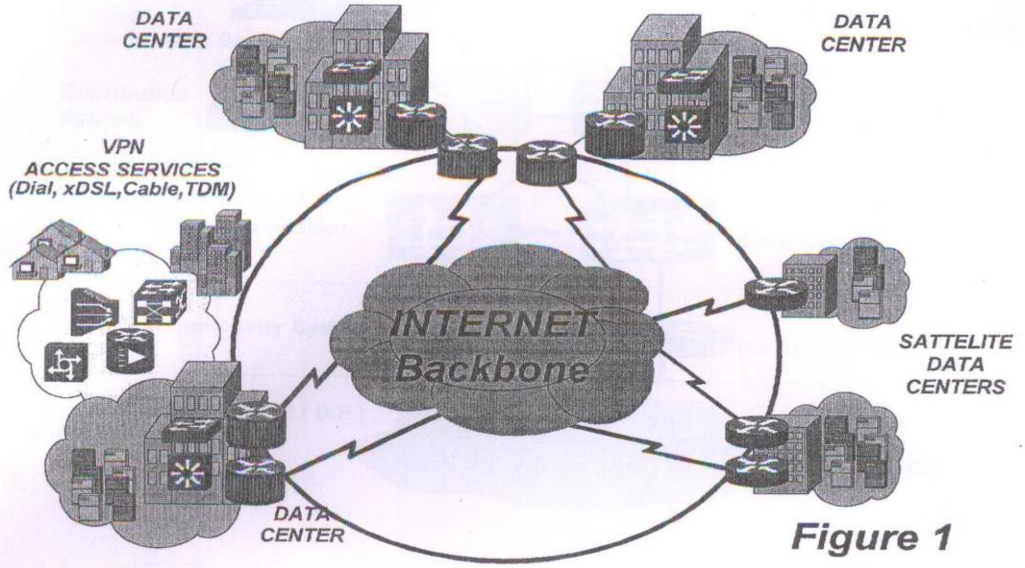

Figure 1

Internet Data Center

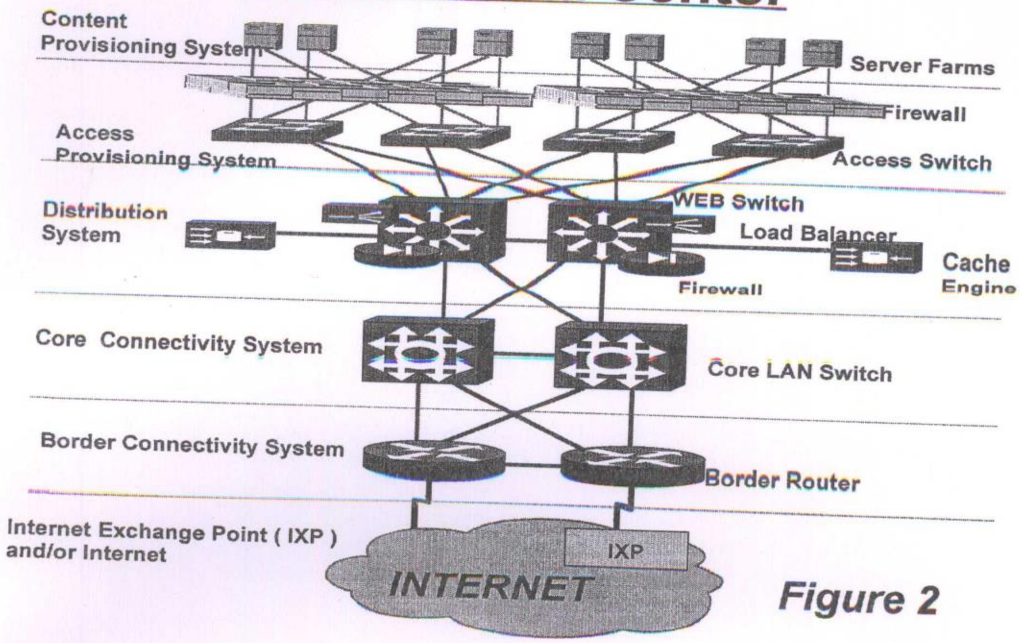

Figure 2