**Annexure 1 – Asset Register Templates**

**1. Hardware Asset Register**

| Equipment | Name/Brand /OEM | Serial No: | Installed Date | FAT/UAT date | Supporting document available for FAT(Y/N) | Warranty | | Location of the Asset | For Switches/routers | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | From | To | | Total Number of Ports | Type of ports | Number of ports utilized |
| Routers | | | | | | | | | | | |
| Switches | | | | | | | | | | | |
| Firewall | | | | | | | | | | | |
| Wireless equipment | | | | | | | | | | | |
| VC equipment( MCU, Cameras, Monitors etc) | | | | | | | | | | | |
| Voice related equipment( Phones, control units, routers etc) | | | | | | | | | | | |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Wireless equipment | | | | | | | | | | | |
| Servers | | | | | | | | | | | |
| UPS | | | | | | | | | | | |

**2. Software Asset Register:**

| Name of the software | Type | Media Serial No: | Installed Date | Warranty | | Asset Physical Location | Number of licenses | Version |
|---|---|---|---|---|---|---|---|---|
| | | | | From | To | | | |
| Operating systems | | | | | | | | |
| Driver CDs, dial up CDs etc | | | | | | | | |
| Monitoring Software | | | | | | | | |
| Any other software | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

**3. Information Asset Register**

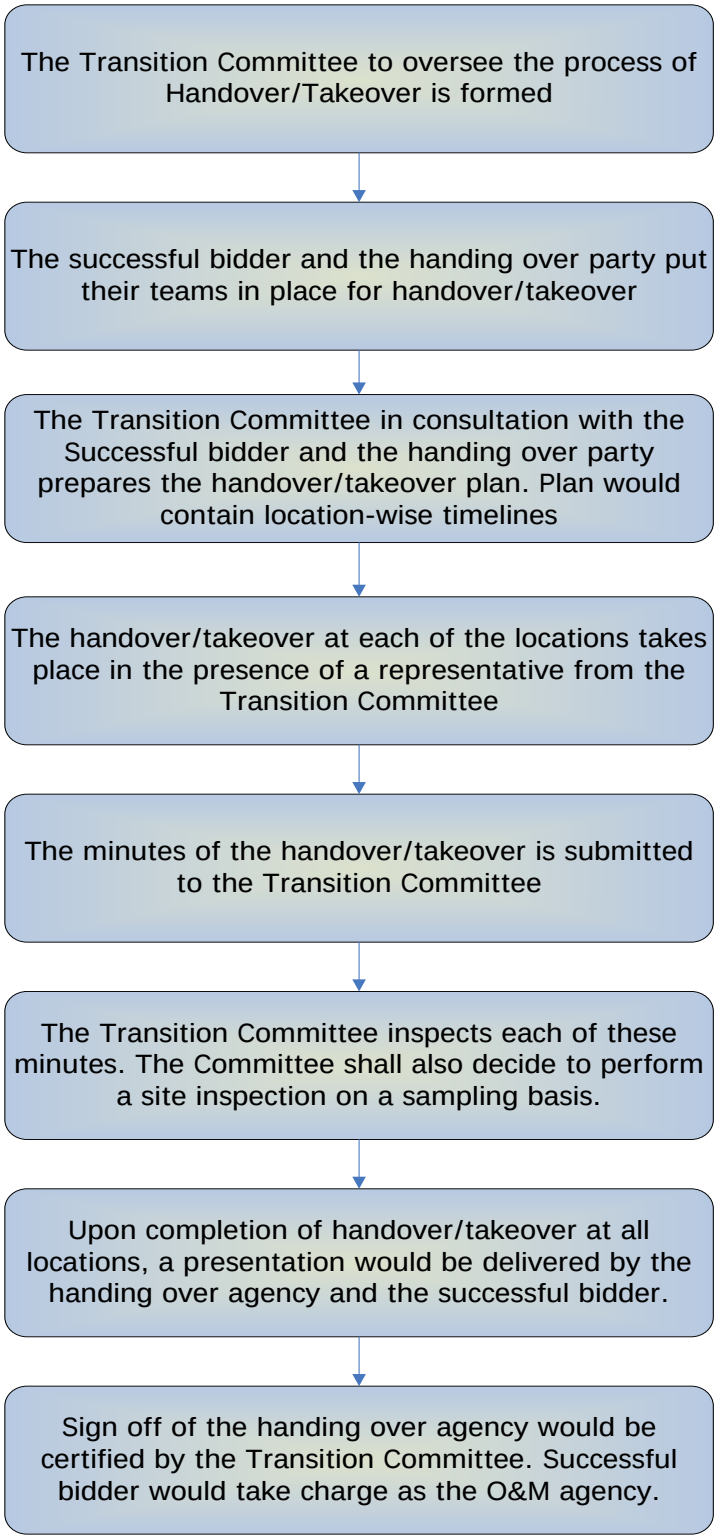
| Information | Type ( Soft copy/ Hard copy) | Asset Physical Location | Approver of Document | Date approved |
|---|---|---|---|---|
| Process documents | | | | |
| Operating manuals for Equipment | | | | |
| Layout Diagrams | | | | |
| Network Topology | | | | |
| User manuals | | | | |
| Do’s and Don’ts Checklist | | | | |
| Operating Checklist | | | | |
| Access Logs | | | | |
| Security Logs | | | | |
| Reports/Returns | | | | |
| Billing invoices | | | | |
| Contract Documents/SLAs | | | | |
| Resource Plan | | | | |

**4. People Asset Register**

| Name | Designation | Role | Responsibility | Qualification | Location | Period Deployed | |
|---|---|---|---|---|---|---|---|
| | | | | | | From | To |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

**Annexure-2 Handover / Takeover Process**

The following chart would depict the processes that shall be involved in this entire handover/takeover exercise.



**Protocol on Handover / Takeover procedure of Duties, Assets and Official Documents**

*1. Handover/takeover should happen only between persons duly nominated*

The bidder would have to nominate specific members from their team for the handover/takeover activity for each of the locations. The bidder should clearly specify as to which team member would be involved in which aspect of the takeover (procedure/documentation/hardware/software etc.). There should be at least two team members (primary and secondary nominees) nominated for each of the takeover procedures. The team nomination should be presented in the following format.

| S. No. | Primary Nominee(s) | Secondary Nominee(s) | Takeover procedure | Description |
|---|---|---|---|---|
| 1. | | | | |
| 2. | | | | |

*2. The handover/takeover procedure shall include the takeover of*

a. Assets

The assets would include software, hardware and networking components. The following is the list of various assets and their type that would require takeover

| S. No. | Asset type | Asset list | Remarks |
|---|---|---|---|
| 1. | Hardware components | | <to be taken from the existing operator> |
| 2. | | | |
| 3. | Network components | | <to be taken from the existing operator> |
| 4. | | | |
| 5. | Software | | <to be taken from the existing operator> |
| 6. | | | |
| 7. | | | |

b. Documentation

The documents that require to be taken over would include user manuals, hardware configuration sheets, reports and templates etc. The following is the list of various documents that would have to be taken over

| S. No. | Document type | Document list | Remarks |
|---|---|---|---|
| 1. | Manuals | | <list to be obtained from the existing O&M agency> |
| 2. | | | |
| 3. | Configuration sheets | | |
| 4. | | | |
| 5. | Performance Reports | | |
| 6. | | | |
| 7. | | | |
| 8. | OEM certificates and warranties | | |
| 9. | Software licenses | | |
| 10. | Software media | | |
| 11. | Reporting Templates (if any) | | |
| 12. | | | |

3. *Handover/takeover procedure should be carried out in the presence of a representative from the Transition Committee*

The entire handover/takeover procedure would have to take place in the presence of the a representative from the official committee that shall be formed for this purpose. This committee, called the Transition Committee. The committee would comprise the following members

| S. No. | Member | Role | Organization |
|---|---|---|---|
| 1. | Representative from DST , Govt. of Gujarat | Chairman | DST, Govt. of Gujarat |
| 2. | Programme Management ,Third party Auditor Consultant | Supervisor | TPA |
| a. | <one from each of the District and Taluka PoPs> | Local coordinator | Representative of local office/organization where POP is located |

*3. Handover/takeover procedure should be carried out in official premises only*

The handover/takeover procedure would have to take place in official premises only. The detailed list of location of handover/takeover would be provided to the successful bidder once the contract is finalized. None of the aforementioned assets/documentations shall be taken outside the premises without prior approval of the handover/takeover committee. Assets/documentation being taken out would have to be recorded in the following format

| S. No. | Asset/ Document Check out | Check out by | Purpose | Date and Time | Approved by | Date Reinstated | Verified by |
|---|---|---|---|---|---|---|---|
| 1. | | | | | | | |
| 2. | | | | | | | |

*4. Handover/takeover procedure should be minuted*

It is understood that the handover/takeover procedure would last multiple sessions. Thus to bring in sufficient clarity and accountability, each of the handover/takeover sessions at each of the locations would have to be minuted by the successful bidder. The minutes shall capture the details of each of the activities that entail during the handover/takeover, the issues that arise, how the issues have been addressed, action points taken and the tentative agenda for the next handover/takeover session. The minute is also required to capture the personnel present during each of the sessions. Following is the recommended format that the bidder shall follow for minuting details of the handover/takeover sessions.

**Handover/takeover session no. <xx>**

**Date :**

**Location :**

**Participants:**

**Transition Committee Representative:**

xxx

**Handover Agency:**

xxx

| **Takeover Agency:** |
| --- |
| xxx |
| **Agenda of the session and Decisions Taken** |
| **1.** |
| **2.** |
| **3.** |
| **4.** |
| **Agenda for the next session:** |
| **Signatures:** |

The minute prepared would have to be submitted to the Transition Committee within one working day after the conclusion of each of the handover/takeover sessions. The minutes would be inspected for consistency by the Transition Committee and shall be issued later and recorded.

**Checklist for Handover/Takeover**

1. Handover/takeover of processes
    a. Operational processes o Yes o No
    b. Security processes o Yes o No
    c. Emergency o Yes o No
    d. Others (specify) o Yes o No
2. Handover/takeover of assets
    a. Servers o Yes o No
    b. Network components o Yes o No
    c. Other IT components o Yes o No
    d. Electrical equipment o Yes o No
    e. Others (specify) o Yes o No
3. Handover/takeover of documents
    a. Manuals o Yes o No
    b. Configuration sheets o Yes o No
    c. Performance Reports o Yes o No
    d. OEM certificates and warranties o Yes o No
    e. Software licenses o Yes o No
    f. Software media o Yes o No
    g. Reporting Templates (if any) o Yes o No
    h. Others (specify) o Yes o No

**Asset Master List** <needs to be revised based on information obtained from the current O&M agency>

| S. No. | Type | Item Description | Number | Date of Handover | Approved by O&M Operator | Date of Approval |
|---|---|---|---|---|---|---|
| 1. | Servers | Web server | | | | |
| 2. | | Application Server | | | | |
| 3. | | Database Server | | | | |
| 4. | | Staging Server | | | | |
| 5. | | Integration Server | | | | |
| 6. | | Unified Messaging Server | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 7. | | Racks | | | | |
| 8. | Network Components | SAN storage | | | | |
| 9. | | Tape library | | | | |
| 10. | | Router | | | | |
| 11. | | LAN Switch | | | | |
| 12. | | Application Switch | | | | |
| 13. | | Firewall | | | | |
| 14. | | SAN Switches | | | | |
| 15. | | Optical Cable Infrastructure | | | | |
| 16. | | Intrusion Detection System | | | | |
| 17. | Other IT Components | Desktops | | | | |
| 18. | | Keyboard and Video Display Unit | | | | |
| 19. | | UPS | | | | |
| 20. | Others | Precision AC | | | | |
| 21. | | Generator Sets | | | | |
| 22. | | Electrical Work | | | | |
| 23. | | Automatic Voltage Regulator | | | | |
| 24. | Software | | | | | |
| 25. | | | | | | |
| 26. | Hardware Configuration sheets | | | | | |
| 27. | | | | | | |
| 28. | Manuals | | | | | |
| 29. | | | | | | |
| 30. | Reports | | | | | |
| 31. | | | | | | |
| 32. | Templates | | | | | |
| 33. | | | | | | |
| 34. | | | | | | |

## *ANNEXURE-3 GUIDELINE FOR NETWORK MANAGEMENT PROCESSES*

For better management of the network. The process to be implemented as elaborated below and should be implemented by the selected O&M operator. The Gujarat State Wide Area Network (GSWAN), should be managed in accordance to various standards e.g. ISO Network Management Model, ITIL etc. It is required that the processes be defined under four major functional areas that would govern the GSWAN Network Management:

1. Configuration management
2. Performance management
3. Fault management

### 1.1 GSWAN Network Management Functional Areas

#### 1.1.1 Configuration Management

The configuration side of GSWAN network management is for tracking the hardware and software versions on the network to identify their effects on the network's operation. An example of this is Microsoft's System Management Server (SMS) which has the capability to monitor, manage and track every piece of software and hardware on a given network.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Fault Management** | **Fault Detection** | **Fault Correction** | **Fault Isolation** | **Network Recovery** | **Alarm Handling** | **Alarm Filtering** | **Alarm Generation** | **Clear Correlation** |
| **Configuration Management** | **Resource Utilisation** | **Network Provisioning** | **Auto and Sub rack Discovery** | **Backup and Restore Database Handling** | **Resource Shutdown** | **Change Management** | **Support For Preprovisionning** | **Inventory Asset Management** |
| **Performance Management** | **Utilisation and error rates** | **Consistent performance level** | **Performance Data Collection** | **Performance report generation** | **Performance Data Analysis** | **Problem reporting** | **Capacity Planning** | **Performance data/statistics collection** |
| **Security Management** | **Selective resource access** | **Enable NE functions** | **Access logs** | **Security Alarm/Event reporting** | **Data Privacy** | **User access rights checking** | **Security breaches and attempts** | **Security audit trail log** |
| **Accounting Management** | **Track service resource usage** | **Cost for services** | **Accounting Limit** | **Combine costs for multiple resources** | **Set quotas for usage** | **Audits** | **Toll fraud reporting** | **Support for different modes of accounting** |

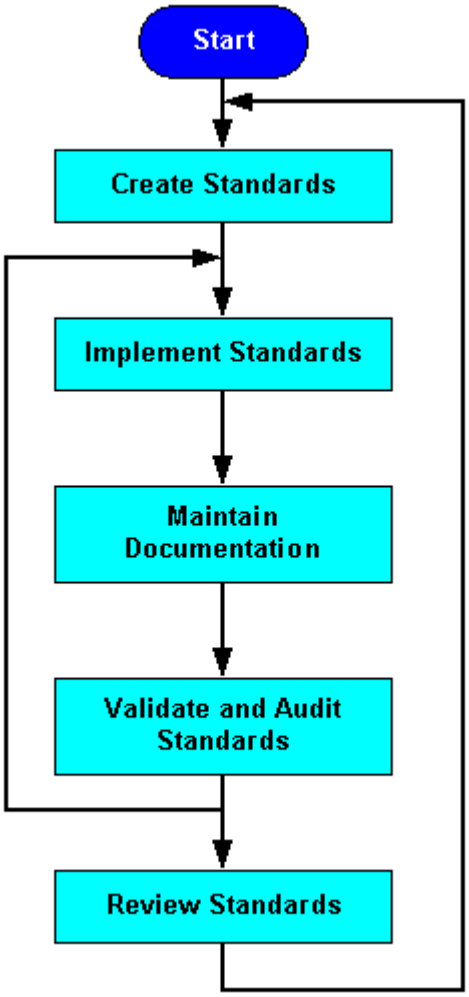
Configuration management is a collection of processes and tools that promote network consistency, track network change, and provide up to date network documentation and visibility. By building and maintaining configuration management best-practices, GSWAN can expect several benefits such as improved network availability and lower costs. These include:

- Lower support costs due to a decrease in reactive support issues.
- Lower network costs due to device, circuit, and user tracking tools and processes that identify unused network components.
- Improved network availability due to a decrease in reactive support costs and improved time to resolve problems.

Following issues generally result from lack of configuration management:

- Inability to determine user impact from network changes
- Increased reactive support issues and lower availability
- Increased time to resolve problems
- Higher network costs due to unused network components

High-Level Process Flow for Configuration Management is indicated in the figure.



The diagram above shows how you can use the critical success factors followed by performance indicators to implement a successful configuration management plan.

## Creating standards

Creating standards for network consistency helps reduce network complexity, the amount of unplanned downtime, and exposure to network impacting events. We recommend the following standards for optimal network consistency:

A. Software version control and management
B. IP addressing standards and management
C. Naming conventions and Domain Name System/Dynamic Host Configuration Protocol (DNS/DHCP) assignments
D. Standard configurations and descriptors
E. Configuration upgrade procedures
F. Solution templates

### *A. Software Version Control and Management*

Software version control is the practice of deploying consistent software versions on similar network devices. This improves the chance for validation and testing on the chosen software versions and greatly limits the amount of software defects and interoperability issues found in the network. Limited software versions also reduce the risk of unexpected behavior with user interfaces, command or management output, upgrade behavior and feature behavior. This makes the environment less complex and easier to support. Overall, software version control improves network availability and helps lower reactive support costs.

Steps to follow for Software version control:

- Determine device classifications based on chassis, stability, and new feature requirements.
- Target individual software versions for similar devices.
- Test, validate, and pilot chosen software versions.
- Document successful versions as standard for similar-device classification.
- Consistently deploy or upgrade all similar devices to standard software version.

### *B. IP Addressing Standards and Management*

IP address management is the process of allocating, recycling and documenting IP addresses and subnets in a network. IP addressing standards define subnet size, subnet assignment, network device assignments and dynamic address assignments within a subnet range. Recommended IP address management standards reduce the opportunity for overlapping or duplicate subnets, non-summarization in the network, duplicate IP address device assignments, wasted IP address space, and unnecessary complexity.

Create standards for IP address assignments within each subnet range, they should be documented and referenced on all network engineering plan documents to help ensure consistent deployment.

### *C. Naming Conventions and DNS/DHCP Assignments*

Consistent, structured use of naming conventions and DNS for devices shall help manage the GSWAN in the following ways:

- Creates a consistent access point to routers for all network management information related to a device.
- Reduces the opportunity for duplicate IP addresses.
- Creates simple identification of a device showing location, device type, and purpose.
- Improves inventory management by providing a simpler method to identify network devices.

### *D. Standard Configuration and Descriptors*

Standard configuration applies to protocol and media configurations, as well as global configuration commands. Descriptors are interface commands used to describe an interface.

Create standard configurations for each device classification, such as router, LAN switch, WAN switch, or ATM switch. Each standard configuration should contain the global, media, and protocol configuration commands necessary to maintain network consistency. Media configuration includes ATM, Frame Relay, or Fast Ethernet configuration. Protocol configuration includes standard IP routing protocol configuration parameters, common Quality of Service (QoS) configurations, common access lists, and other required protocol configurations. Global configuration commands apply to all like

devices and include parameters such as service commands, IP commands, TACACS commands, vty configuration, banners, SNMP configuration, and Network Time Protocol (NTP) configuration.

### *E. Configuration Upgrade Procedures*

Upgrade procedures help ensure that software and hardware upgrades occur smoothly with minimal downtime. Upgrade procedures include vendor verification, vendor installation references such as release notes, upgrade methodologies or steps, configuration guidelines, and testing requirements.

Upgrade procedures may vary widely depending on network types, device types, or new software requirements. Individual router or switch upgrade requirements may be developed and tested within an architecture group and referenced in any change documentation. Other upgrades, involving entire networks, can not be tested as easily. These upgrades may require more in-depth planning, vendor involvement, and additional steps to ensure success.

### *F. Solution Templates for Departmental Network Expansion*

Create solution templates for all network deployments and solutions that will be deployed more than once, e.g. expansion for any departments. The solution template contains all standard hardware, software, configuration, cabling, and installation requirements for the network solution. Specific details of the solution template are shown as follows:

- Hardware and hardware modules including memory, flash, power, and card layouts.
- Logical topology including port assignments, connectivity, speed, and media type.
- Software versions including module or firmware versions.
- All non-standard, non device-specific configuration including routing protocols, media configurations, VLAN configuration, access lists, security, switching paths, spanning tree parameters, and others.
- Out-of-band management requirements.
- Cable requirements.
- Installation requirements including environmental, power, and rack locations.

## **Maintain Documentation**

Document the network and changes that have occurred in the network in near real-time. This precise network information can be used for troubleshooting, network management

tool device lists, inventory, validation, and audits.For this purpose ,use following network documentation critical success factors:

- Current device, link, and end-user inventory
- Configuration version control system
- TACACS configuration log
- Network topology documentation

**Validate and Audit Standards**

Configuration management performance indicators provide a mechanism to validate and audit network configuration standards and critical success factors. By implementing a process improvement program for configuration management, you can use the performance indicators to identify consistency issues and improve overall configuration management.

**Review standards**

Create a cross-functional team to measure configuration management success and improve configuration management processes. The first objective of the team is to implement configuration management performance indicators in order to identify configuration management issues. The following configuration management performance indicators can be defined:

- Configuration integrity checks
- Device, protocol, and media audits
- Standards and documentation review

Carry out monthly audits, or possibly quarterly if only validation is needed. Review past audits to confirm that past problems are resolved. Look for overall improvements and goals to demonstrate progress and value. Create metrics to show the quantity of high-risk, medium-risk, and low-risk network configuration inconsistencies.

### 1.1.2 Performance Management

Performance management is monitoring, assessing, and adjusting the available bandwidth and network resource usage in order make a network run more efficiently. Performance management is a **very** important part of the network management model particularly to the Government of Gujarat and/or departments, that wants to utilize the GSWAN network and streamline their network's performance.

Performance management involves optimization of network service response time and management of the consistency and quality of individual and overall network services. The most important service is the need to measure the user/application response time. For most users, response time is the critical performance success factor. This variable shapes the perception of network success by both your users and application administrators.

1. Define and document Network Management Objective
    a] Document: Services, Scalability and Availability Objectives
    b] Define SLAs and SLA catalogues

2. Measure Performance
    a] Gather Network Baseline Data
    b] Measure Availability
    c] Measure Response Time
    d] Measure Accuracy
    e] Measure Utilization
    f] Capacity Planning

3. Perform a Proactive Fault Analysis
    a] Use Thresholds for Proactive Fault Management
    b] Network Management Implementation
    c] Network Operation Metrics

**Define and document Network Management Objective**

Document the goals for the GSWAN and supported services in a way that all users can understand. These are the standard performance goals:

- Response time
- Utilization
- Throughput
- Capacity (maximum throughput rate)

**Measure Performance**

Performance management is an umbrella term that incorporates the configuration and measurement of distinct performance areas. This section describes these six concepts of performance management:

- Gather Network Baseline Data
- Measure Availability
- Measure Response Time
- Measure Accuracy
- Measure Utilization
- Capacity Planning

**Gather and maintain GSWAN Baseline Data**

Perform a baseline of the current GSWAN prior to a new solution (application or IOS change) deployment and after the deployment in order to measure expectations set for the new solution. This baseline helps determine if the solution meets performance and availability objectives and benchmark capacity. A typical router/switch baseline report includes capacity issues related to CPU, memory, buffer management, link/media utilization, and throughput. There are other types of baseline data that one might also include, based on the defined objectives in the concept of operations. For instance, an availability baseline demonstrates increased stability/availability of the network environment. Perform a baseline comparison between old and new environments in order to verify solution requirements.

**Measure Availability**

One of the primary metrics used by network managers is availability. Availability is the measure of time for which a network system or application is available to a user. From a network perspective, availability represents the reliability of the individual components in a network.

For example, in order to measure availability, one might coordinate the help desk phone calls with the statistics collected from the managed devices. However, availability tools cannot determine all of the reasons for failure.

Network redundancy is another factor to consider when one measures availability. Loss of redundancy indicates service degradation rather than total network failure. The result might be slower response time and a loss of data due to dropped packets. It is also possible the results show up in the other areas of performance measurement such as utilization and response time.

**Measure Response Time**

Network response time is the time required for traffic to travel between two points. Response times slower than normal, seen through a baseline comparison or that exceed a threshold, might indicate congestion or a network fault.

Response time is the best measure of customer network use and can help you gauge the effectiveness of your network. No matter what the source of the slow response is, users get frustrated as a result of delayed traffic. In distributed networks, many factors affect the response time, such as:

- Network congestion
- Less than desirable route to destination (or no route at all)
- Underpowered network devices
- Network faults such as a broadcast storm
- Noise or CRC errors

Whenever possible, oyou should measure response time as it appears to users. A user perceives response as the time from when they press Enter or click a button until the screen displays. This elapsed time includes the time required for each network device, the user workstation, and the destination server to process the traffic.

**Measure Accuracy**

Accuracy is the measure of interface traffic that does not result in error and can be expressed in terms of a percentage that compares the success rate to total packet rate over a period of time. One must first measure the error rate. For instance, if two out of every 100 packets result in error, the error rate would be 2% and the accuracy rate would be 98%.

With earlier network technologies, especially in the wide area, a certain level of errors was acceptable. However, with high-speed networks and present-day WAN services, transmission is considerably more accurate, and error rates are close to zero unless there is an actual problem. Some common causes of interface errors include:

- Out-of-specification wiring
- Electrical interference
- Faulty hardware or software

Use a decreased accuracy rate to trigger a closer investigation. One might discover that a particular interface exhibits problems and decides that the errors are acceptable. In this case, one should adjust the accuracy threshold for this interface in order to reflect where the error rate is unacceptable. The unacceptable error rate might have been reported in an earlier baseline.

**Measure Utilization**

Utilization measures the use of a particular resource over time. The measure is usually expressed in the form of a percentage in which the usage of a resource is compared with its maximum operational capacity. Through utilization measures, one can identify congestion (or potential congestion) throughout the network. One can also identify underutilized resources.

Utilization is the principle measure to determine how full the network pipes (links) are. Measure CPU, interface, queuing, and other system-related capacity measurements in order to determine the extent to which network system resources are consumed.

High utilization is not necessarily bad. Low utilization might indicate traffic flows in unexpected places. As lines become over utilized, the effects can become significant. Over utilization occurs when there is more traffic queued to pass over an interface than it can handle. Sudden jumps in resource utilization can indicate a fault condition.

### 1.1.3 Fault Management

The goal of fault management is to detect, log, notify users of, and (to the extent possible) automatically fix network problems to keep the network running effectively. Because faults can cause downtime or unacceptable network degradation, fault management is perhaps the most widely implemented of the ISO network management elements.

**Perform a Proactive Fault Analysis**

Proactive fault analysis is essential to performance management. The same type of data that is collected for performance management can be used for proactive fault analysis. However, the timing and use of this data is different between proactive fault management and performance management.

Proactive fault management is the way that the ideal network management system can achieve the determined goals . The relation to performance management is through the baseline and the data variables that are uses. Proactive fault management integrates customized events, an event correlation engine, trouble ticketing, and the statistical analysis of the baseline data in order to tie together fault, performance, and change management in an ideal, effective network management system.

**Use Thresholds for Proactive Fault Management**

Thresholding is the process in which one define points of interest in specific data streams and generate events when thresholds are triggered. Use one network performance data to set those thresholds.

There are several different types of thresholds, some of which are more applicable to certain types of data. Thresholds are only applicable to numeric data so convert any textual data into discrete numeric values. Even if one does not know all of the possible text strings for an object, one can still enumerate the "interesting" strings and assign all other strings to a set value.

**Annexure-4 Guidelines and Best practices for Connectivity**

**Recommendations for Horizontal Connectivity**

The following guidelines can be adopted to provide for an efficient, scalable and flexible network.

1. As hierarchical topology has advantages of better scalability, manageability, ease of troubleshooting, ease of implementation, protocol support and predictability, the same can be utilized for horizontal connectivity.

2. As Ahmedabad is part of the Mesh Ring District Network Cluster it would have one router (7609) dedicated for forming the ring with other district clusters. This same router could be used as the core for district horizontal connectivity.

3. Within the district based the departmental offices could be clubbed together to form 4 regional clusters/BTS based on the distances between the offices.

4. A layer 2 manageable switch can be used to form these regional clusters which get connected in a ring mesh topology. Alternately BTS stations could be set up for an RF network for horizontal connectivity within these clusters.

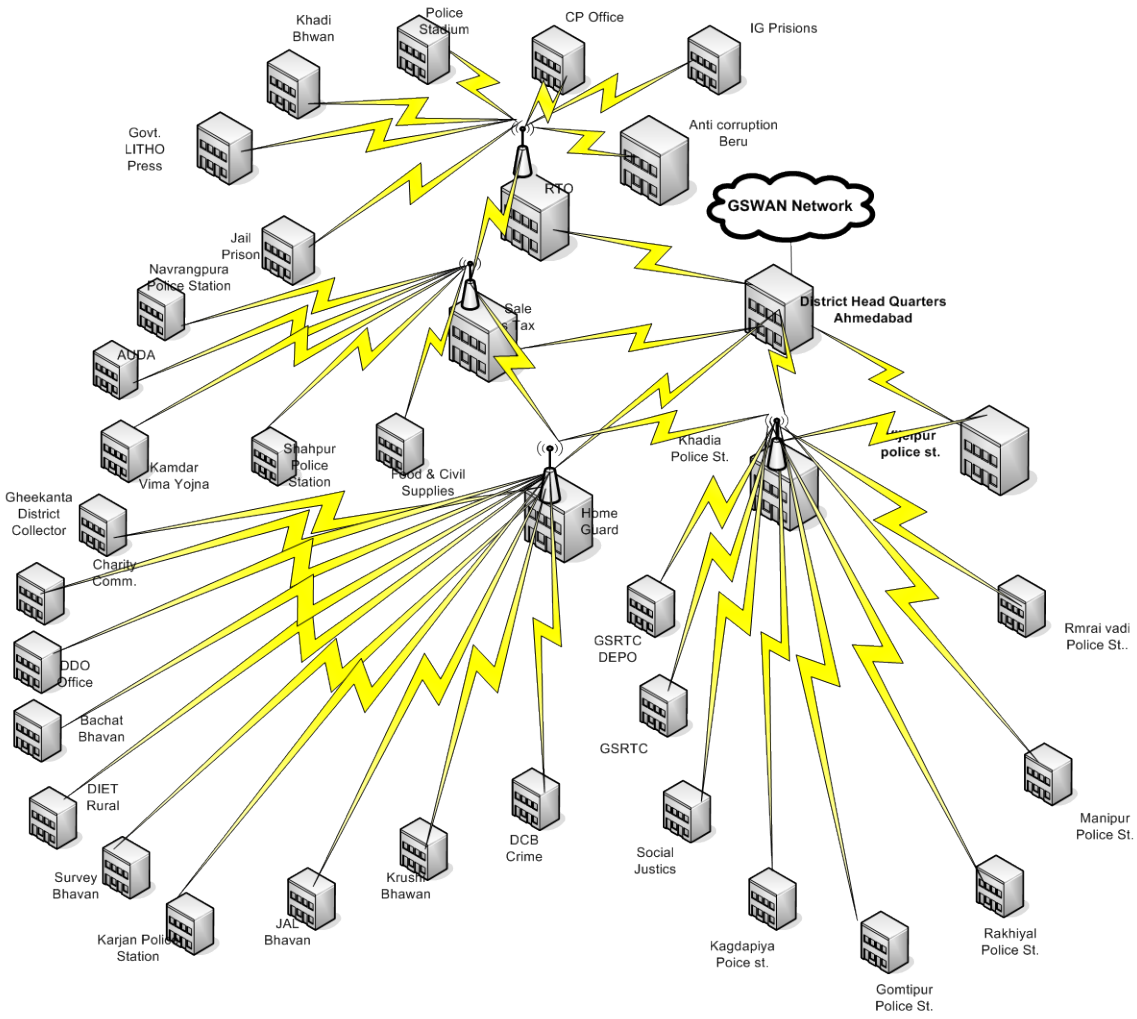
5. Assuming that at any given time there would be a requirement of providing concurrent video, voice, data connectivity to minimum 8 offices, a minimum of 4 Mbps bandwidth uplink (could be divided into a pair of 2 mbps uplinks)from regional clusters to the core router at Ahmedabad PoP would be required.

6. The core router at Ahmadabad PoP(7609) further could get connected to the core router at SHQ with an 8 Mbps link.

7. The above scenario has been depicted in the fig given below. As the links/connectivity is necessarily required to cater to voice, video and data streaming it is advisable to either go for dedicated lease lines or ISDN, PRI(Primary rate interface) E1 standard.

8. On similar lines the other districts within the 6 clusters/rings could be connected for horizontal connectivity.

9. For horizontal connectivity at Talukas layer 2 unmanaged switches could be used at taluka offices with a requirement of more than 10 nodes, which in turn could get connected directly to the router 1751. Alternately, if the number of offices to be connected is less, they could get connected through VLAN on the router itself.


Khadi Bhwan
Police Stadium
CP Office
IG Prisions
Govt. LITHO Press
Anti corruption Beru
RTO
GSWAN Network
Jail Prison
Navrangpura Police Station
Sale Tax
District Head Quarters Ahmedabad
AUDA
Kamdar Vima Yojna
Shahpur Police Station
Food & Civil Supplies
Khadia Police St.
Home Guard
Gheekanta District Collector
Charity Comm.
DDO Office
Bachat Bhavan
DIET Rural
Survey Bhavan
Karjan Police Station
JAL Bhavan
Krushi Bhawan
DCB Crime
GSRTC DEPO
GSRTC
Social Justics
Kagdapiya Poice st.
Gomtipur Police St.
Rakhiyal Police St.
Manipur Police St.
Rmrai vadi Police St..

**Recommendations for GSWAN Vertical Connectivity**

At present under the GSWAN enhancement scheme the initial bottle necks created by the star topology for connectivity of 25 DHQs to the SHQ has been revised to form a ring mesh based cluster network consisting of six rings/clusters.

Following are key recommendations for vertical connectivity:

1. A hierarchical topology is again recommended for vertical connectivity from SHQ to DHQ to THQs.

2. As of the Mesh Ring District Network Cluster it would have one router (7507) dedicated for connectivity to Taluka headquarters. This same router could be used as the core for hierarchical connectivity down to the THQ PoPs.

3. The ring mesh topology designed at District level can be replicated at the taluka level clubbing talukas within a district, based on the proximity to form of taluka clusters within a district.

4. Here again assuming the example of Ahmadabad district for 11 Talukas, 2 clusters could be created.

5. Assuming that at any given time there would be a requirement of providing concurrent video, voice, data connectivity to all Taluka headquarters a minimum of 5 Mbps bandwidth uplink would be required from the regional Taluka clusters.

6. To cater for redundancy it would be advisable to provide 2 uplinks, one 4 Mbps each, for connectivity to District PoP(7507), with load balancing feature at the regional cluster.

7. The existing CISCO 1751 router at the taluka headquarters could be used with expansion slots to form these regional clusters which get connected in a ring

mesh topology. Alternately even BTS stations could be used for forming some clusters based on an RF network.

## 1.1 Guidelines for LAN within multi-storied buildings

### Introduction

The following set of guidelines have to be used for the development of robust networking infrastructures within multi-storied buildings. The purpose of these guidelines is to minimize the DST investment by maximizing the efficiency of the network and minimizing outages while minimizing the staff necessary to provide the facilities and services.

A multi-storied building's networking infrastructure involves a number of hardware components including wiring, connectors, racks, network interface cards, client and server workstations, and communications devices such as repeaters, bridges, switches, and routers. It also includes software such as network card drivers, communications protocols, network operating systems and network application tools. This document focuses on the entire range of these components.

Although Ethernet, OFC and RF networks are deployed on the GSWAN, the predominant networking technology is Ethernet. The predominance of Ethernet at GSWAN is mirrored in the deployment of networking infrastructures worldwide, and networking vendors continue to develop faster and better Ethernet products. Therefore, this document will focus exclusively on guidelines for Ethernet networking, and it is strongly recommended that all new infrastructures on the GSWAN campus be based on Ethernet for the aforementioned reasons.

### Wiring guidelines for multi-storied buildings

The guidelines are as follows

1. Even if multi-storied building networks have implemented Ethernet cabling technologies, the desirable implementation strategy is to deploy structured wiring using fiber optic cabling for building backbones and CAT 5 / CAT 6 UTP cabling to connect end devices. Wiring for new and renovated buildings must comply with standard wiring specifications. In particular, these specifications require that for all

new and renovated buildings, any proposed building wiring designs be approved by competent authority prior to installation. The deployment of data wiring in existing buildings should also adhere to these specifications whenever possible.

2. All network components and wiring racks must be properly grounded. EIA/TIA 606 is the administration standard for telecommunications infrastructure and should be followed. This specification covers cable labeling, telecommunications records, required drawings, and a method of knowing who to contact for each part of the infrastructure. Each of these standards has been condensed into a small pamphlet, which most networking vendors can provide.
3. Structured wiring, which uses a star topology, has a number of advantages over thick and thin coaxial Ethernet infrastructures which utilize bus topologies.

a. First, it is easier to add, move, or change connections by moving patch cables in a wiring closet.
b. Second, troubleshooting is easier and less time consuming since one can quickly disconnect network devices in the wiring closet rather than having to go to each workstation (or get into the ceiling) to disconnect malfunctioning devices; some vendor management software can isolate and eliminate network problems as they occur and notify the network administrator of the problem.
c. Third, workstations do not have to be powered down before making a cable switch, as they do in a thick coaxial infrastructure. In addition, the cable failure of one networked device does not generally affect others.
d. Finally, new connection capacity can be added by installing additional switch devices in the wiring closet.

4. It is advised that Cat 6 UTP cabling, which is also the industry standard is used to connect a networked device to the wiring closet. It can support data rates up to 1000 Mbps using sophisticated encoding methods and will likely support local area network (LAN) traffic for the next 10 to 15 years, even though the active network components will have to be replaced in a much shorter time span to provide increased bandwidth and services.
5. Category 5e cabling may be employed when incremental additions to existing Category 5e cabling for major cable plant modifications and/or additions due to building renovations or remodeling are necessary. Category 6 link and channel requirements are backward compatible to Category 5e.

6. Fiber Network Cabling: Structured Cabling System installations for new multi-storied buildings, major cable plant additions or modifications, building renovations or remodeling shall be either multi-mode or single-mode, depending on business unit requirements, as specified by TIA/EIA 568-B.3 and ISO/IEC 11801:2002 Commercial Building Telecommunications Cabling Standards.

a. TIA/EIA-568-B series standards specify 50/125 micron multi-mode fiber for horizontal subsystems. 50/125 micron multi-mode or single-mode (8/125 micron) fiber is specified for vertical subsystems.

- Multi-mode fiber transmits up to 10 Gbps Ethernet a distance of approximately 35 meters to 300 meters (50/125 micron), depending on the specific fiber and the Ethernet port characteristics. Single-mode (8/125 micron) transmits up to 10 Gbps Ethernet a distance of 2, 10, and 40 kilometers, depending upon specifications.
- Single-mode fiber network cabling subsystems between buildings allow up to 10-Gbps Ethernet transmission rates over greater distances, as specified by the International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) Series G.652 and ISO/IEC 60793 standards.

<u>Wiring guidelines pertaining to network design have been elaborated below:</u>

7. In order to minimize costs over the long term, it is highly desirable to develop a comprehensive building network design that takes into account the needs of all of the building occupants. Once that design has been developed, it can be implemented in phases as funding permits. Departments are strongly encouraged to seek the assistance of professional network designers, rather than design the network themselves, before implementing a new networking infrastructure. The GSWAN Network Operations Center (NOC) is one such source for professional design assistance. If a department insists on developing its own design, there are a number of concepts and issues that need to be understood before proceeding.
8. Building networks that adhere to structured wiring specifications typically have one central wiring closet called a main distribution frame (MDF) and one or more distributed wiring closets called intermediate distribution frames (IDFs). It is highly desirable to secure the MDF and IDFs behind locked doors, and they should be large enough to support all of the equipment with sufficient room to reach all devices in

them. These facilities should also adhere to the standard environmental specifications that are currently prevalent.

9. Each IDF should be star wired back to the MDF via fiber optic cabling. Fiber cabling supports longer distances (2,000 meters for multi-mode fiber) than twisted pair copper wiring, and it is immune to electrical interference and grounding problems. It also has the potential for supporting high data transmission capacities (gigabits per second). Twelve strands of fiber cabling should be run from MDF to each IDF to provide for future growth and redundancy.
10. Networked devices, such as microcomputer workstations, connect to IDFs through star wired CAT 6 UTP. One CAT 6 cable should be installed for each networked device in a room location with at least one additional CAT 6 cable installed for growth and redundancy. It is best to locate an IDF in a central location on a floor, when possible, to limit the number of IDFs per floor. In addition, it would be ideal for the IDFs on each floor to be stacked on top of one another to minimize backbone cable paths.
11. The LAN components of an IDF minimally consist of one or more rack mounted switches (either modular chassis or stackable, shared and/or switched) with each switch port connecting to a port on a rack mounted patch panel via a **stranded wire** CAT 6 UTP patch cable. Each port on the patch panel is connected to an RJ-45 wall plate in an office through a **solid conductor** horizontal CAT 6 UTP cable running through the building infrastructure. The networked device is connected to the wall plate via a **stranded wire** CAT 6 UTP station cable.
12. The total cable length for CAT 6 UTP wiring is 100 meters (90 meters for horizontal cabling and 10 meters for both station and patch cables combined). As indicated above, fixed horizontal cables **must** use solid copper CAT 6 wire, whereas, patch cables **must** be stranded copper CAT 6 wire. When designing and installing CAT 6 wiring, it is important to stay away from sources of electrical interference, e.g., 12 inches from light ballasts and four feet from electrical devices such as high-voltage transformers, electric motors, microwave ovens and Xerox machines. Cable trays, which look like metal ladders, can be installed above ceilings to provide clearly defined paths for horizontal CAT 6 wiring, and can keep cables from sources of electrical interference. They also protect cables from damage by other personnel working in ceilings.

13. Rack mounted patch panels are ideal, direct termination points for CAT 6 wiring in the IDF. Although CAT 6 cabling can be terminated in 110-type punch down blocks, it is not recommended unless that type of termination block will be installed for both telephone and data services. Under no circumstances should 66-type punch down blocks be utilized since they can adversely affect data signals. One should also **not** plan to allow two signals (either LAN-LAN or LAN-voice) within the same four pair of a CAT 6 cable, since the signals may interfere with one another.

    Wiring installation related guidelines can be found below

14. Department is **strongly encouraged** to hire qualified professionals to install and terminate cable. The GSWAN and Key Services Vendor can install both CAT 6 and fiber optic cabling. The GSWAN NOC can oversee the installation process. If a department insists on installing their own CAT 5 cable (fiber optic cable requires special equipment and considerable experience to install), they are encouraged to attend professional cable installation training classes. They should also bear in mind the following installation issues.
15. When horizontal CAT 6 cabling is pulled, the maximum pulling tension is 25 lbs. Ivory soap and water can be used to pull cable through conduit, when utilized. Don't allow cables to kink and insure that the **minimum** bending radius is one inch throughout (if one wrapped a CAT 6 cable around a cylindrical object, the radius of the cylinder should minimally be one inch). Cable ties should be loosely attached to avoid pinching the wires. Remember to stay clear of electrical interference, and use cable trays whenever feasible.
16. When terminating CAT 6 cables, make sure that the cable jacket stays on the cable until the end, and allow a **maximum** untwist of only one-half inch. Correct RJ-45 connectors should be utilized (stranded connectors for stranded wire, solid ones for solid wires), and the same pin configuration (or wire map) should be used throughout with correct color codes. At GSWAN the wire map standard should be EIA/TIA 568B.
17. Patch cables should be installed in a neat and orderly fashion. Use cable management guides (brackets and D rings), and cut patch cables to length to avoid dangling, messy loops. If the patch panel serves different sections of the building, one can optionally use different colored patch cables for each section.

18. It is **vitally important** to accurately document the installation, whether professional cable installers or departmental staff are utilized. Before any cabling is installed, one should obtain accurate copies of building blueprints and document the end points (room and IDF) and path of all horizontal CAT 6 and fiber optic cable runs. Each port on the patch panel should have the same **unique** label as the wall plate port in a room. Both ends of the patch cable should also have an identical, **unique** label. In addition, one should maintain a database that minimally maps the patch panel/wall plate port label to a room location and includes the corresponding label for the patch cable as well as a unique switches port number (usually specified through management software).
19. Cable installations must comply with appropriate building codes. All penetrations through fire walls, ceilings and floors must be fire sealed. Many of the older buildings on campus contain asbestos, and installers should obtain training from Public Safety regarding asbestos precautions before drilling holes to potentially avoid installation delays. Plenum rated cable should always be utilized, but it is required when installed in air plenums. Riser rated cable should also be used where required. Furthermore, cables and switches components should be appropriately grounded. If there are any questions regarding building codes, one can contact Campus Planning or the GSWAN NOC in Public Safety. Questions regarding proper grounding techniques can be referred to the GSWAN NOC.
20. Before attaching networking equipment to the cable infrastructure, it is important that each terminated wire is checked with CAT 6 certification equipment (tester/ Analyzer). The equipment should test and document:
    a. The wiring map or pin out to insure that the EIA/TIA 568B map is followed
    b. The signal attenuation through the cable (less than 24.0 dB)
    c. The cable length measurements
    d. Near end crosstalk (NEXT) in both directions (greater than 27.1 dB)

**Wireless guidelines for multi-storied buildings**

Wireless networks Shall be secure, use encryption technologies; be protected using Virtual Private Network (VPN) and firewalls, as necessary; and be compliant with IEEE 802.11x (Wireless Local Area Network (WLAN)), IEEE 802.15 (Wireless Personal Area Network (WPAN)), and IEEE 802.16 (Wireless Metropolitan Area Network (WMAN)).

- Security is to be addressed in the transmission layer with the IEEE 802.11i standard and at the IP applications layer with standards- and policy-based authentication and access control. The WiFi Protected Access (WPA) standard and Protected Extensible Authentication Protocol (PEAP) with the IEEE 802.1x Network Port Authentication standard provides interim, improved security until approval and widespread adoption of 802.11i. In addition, vendor-specific, proprietary, security solutions may provide more enhanced interim security prior to approval and widespread adoption of 802.11i.
- Mobile IP provides an efficient and scalable mechanism to allow users to seamlessly roam among wireless networks. Using Mobile IP in applications such as VoIP, media streaming, and virtual private networking can be supported without service interruption when users move across network boundaries.
- Wireless Profiled TCP (WP-TCP) provides connection oriented services for developing applications that operate over wireless communication networks via the Wireless Application Protocol (WAP). Wireless Profiled TCP is optimized for wireless environments due to the emergence of high-speed wireless networks (e.g., 2.5G and 3G) and provides for large data transfers, end-to-end security (using TLS) and convergence with IETF protocols.
- Wireless client platforms utilizing VPN technologies to access internal networks and mission-critical software applications improve security and decrease certain vulnerabilities inherent in unprotected wireless connectivity.
- Firewall technologies must be implemented at connection points between wireless and wire-based LANs additionally to reduce unauthorized access to internal networks.
- The IEEE 802 standards enable convergence of technologies and the development of an open-standards-based infrastructure for the Wireless Internet.
- The IEEE 802.11x standards form a family of specifications that define how WLAN equipment should be produced so equipment from different manufacturers can work together.
- The IEEE 802.11g is backwards compatible with .11b allowing .11g and .11b devices to coexist in the same network (.11g devices' performance declines based on distance and number of wireless devices).
- The IEEE 802.11f Inter Access Point Protocol ensures interoperability between access points from multiple manufacturers.

- The IEEE 802.15.3 standard is designed for short-range (up to 50 m), very-low-power operation from 11 to 55 Mbps. The standard will provide quality of service, connection management, and advanced power management modes. The IEEE 802.15.2 standard addresses coexistence between WLANs and WPANs operating in the 2.4 GHz frequency band.
- The IEEE 802.16x standards address the “first mile/last mile” connection broadband wireless access for Metropolitan Area Networks, providing up to 155 Mbps transmission speeds. These standards provide for interoperability and coexistence of fixed broadband wireless access systems from multiple manufacturers in both licensed and unlicensed frequency bands. The IEEE 802.16x standards provide for quality of service to support the needs of different applications. IEEE 802.16 WMAN can coexist with IEEE 802.11x WLAN to provide a viable, last-mile, backhaul solution.
- The IEEE 802.17x standards address the Resilient Packet Ring which can handle multiple gigabit transmission speeds in opposite directions. This dual ring technology can be used in MAN and WAN networks.

**Network Devices Guidelines for multi-storied buildings**

**About**

Ethernet started as a shared networking media, i.e., all devices attached to the same physical network (backbone cable) and shared the 10/100/1000 Mbps bandwidth among each other. Devices shared the bandwidth by detecting "collisions" (two or more devices trying to communicate at the same time), backing off, and attempting communications again at a later time. Repeaters, which are devices used to extend cable segments by "repeating" the electrical signals seen on its connected segments, also propagate collision information. The set of devices (network interface cards, cables, and repeaters) connected in this manner is sometimes referred to as a "collision domain".

Shared Ethernet Switches are multi-port repeaters that connect Ethernet devices in a star-wired fashion to the same collision domain. As the number of Ethernet devices within a collision domain increases, the amount of bandwidth available per device decreases.

Since broadcast and multicast frames can harm network performance, routers can be used to isolate these frames and their associated broadcast domains. Unlike bridges which make forwarding decisions based upon media access control (MAC) addresses, routers make forwarding decisions based upon higher-level network protocol (e.g., IP, IPX, AppleTalk) addresses. Working in conjunction with routers, virtual LANs (VLANs) involve relatively new methods of creating artificial broadcast domains by employing software on Ethernet switches to group devices connected to a set of ports in some logical fashion.

**Purpose**

The goal of this section is to help provide guidelines on when and how to connect networked devices in a multi-storied building to the same collision domain (shared switches) or to the same broadcast domain (switched switches and VLANs). When designing a LAN infrastructure one attempts to optimize performance, especially user perception of performance, while minimizing costs. In this event a combination of shared and switched media (and possibly both modular chassis and stackable switches) may give the best bang for the buck.

Note: Please be mindful of the following

1. It should not be forgotten that the newest, fastest, most expensive Ethernet LAN equipment will not necessarily improve services located on other networks. When the LAN is being designed it should be kept in mind that one can really only optimize performance for clients local to the LAN using services local to the same LAN
2. Do not forget that the LAN infrastructure that is being designed is not a short term one and that it is to star for a sufficient large amount of time. It would not be desirable to replace the LAN infrastructure in just a couple of years. Consider possible growth in the number of clients and local services on your LAN as well as the level of bandwidth needed by the local services a few years into the future.

**Network Devices (routers, switches, firewalls, access servers, etc.):** Shall be securely deployed in accordance with applicable IT security standards, and manageable with Network Management platforms that use the most currently approved, open,

industry-standard versions of Simple Network Management Protocol (SNMP) and Remote Monitoring (RMON).

- Backup-up generator power systems and/or Uninterruptible Power Supplies (UPS) protect network devices against loss of electrical power that could disrupt service delivery of mission-critical applications and converged services. Such devices shall be managed and network-connected to protect routers, LAN switches and VoIP/IPT systems. UPS systems should include Ethernet-based network management cards capable of SNMP monitoring via TCP/IP.
- Environmental facilities (air conditioning, humidity controls, etc.) maintain acceptable operating ranges derived from applicable manufacturers' specifications.
- SNMP and RMON facilitate the exchange of management information between network devices as well as network performance management, isolation and analysis of network problems, and growth planning.
- Managed network devices help to ensure the continuous delivery of e-government services and internal business processes.

**LAN Models**

This is an attempt to establish a "rule of thumb" guide to the LAN infrastructure needed to provide optimal connectivity based on four different models or classes of LAN likely to be found at GSWAN. The intent being that knowing which model one's LAN most closely resembles will provide a first step toward what type of and how much LAN equipment is needed. The focus will be on Ethernet LAN equipment, the most commonly used medium at GSWAN.

Note:

Please note that the list of models elaborated below is not completely discrete. Any LAN may resemble more than one model. In this case it is advised that one opts for the higher performance infrastructure.

**Criteria:**

The following are the criteria that help determine the appropriate LAN model

- Location of service(s), local or non-local
- Number of local services
- Distribution of clients to local services
- Bandwidth needed by services
- Number of networked devices

**Definitions:**

The following information would help in defining which is low, medium or high which shall be critical in deciding the selection of a LAN model.

- **Low, medium, and high bandwidth services:** Text E-mail, Telnet, and character based WWW services will be considered to use low bandwidth. Graphical WWW, network file and printer sharing, and FTP are medium bandwidth services. Application sharing (possibly medium bandwidth), high quality voice and video, virtual reality, GIS, and non-client/server databases that use the network as a bus are high bandwidth services.
- **Low, medium, and high numbers of networked devices:** up to about 25 devices = low, 26 - 100 = medium, 100+ = high.
- **Low, medium, and high bandwidth connections:** Shared 10Mbps = low, Switched groups of Shared 10Mbps and Switched 10Mbps = medium, Switched (and Switched Duplexed) 100Mbps = high.

**Models:**

1) Non-local service(s)

This is the scenario in which all the client workstations access a service(s) non-local to the LAN. Such clients may well be able to be optimized using shared 10Mbps media depending upon both the bandwidth required by the services and the number of networked devices. In either case the bottleneck is likely to be non-local to the LAN and as such there may be little that can be done to optimize performance locally.

If the LAN currently most resembles this model it may be advisable to think hard on which model your LAN is most likely to resemble three years from now.

2) One or few local services used by all LAN clients

In this scenario all clients of the LAN access one or more (but not many) local services. In this case LAN performance can be optimized by providing high bandwidth connections, e.g. 100Mbps switched (and possibly duplexed) connections to the services and improved connections, e.g. switched 10Mbps connections, to the clients depending on the service provided and number of networked devices on the LAN.

3) Multiple local services used by respective subsets of clients

This situation can be referred to as a workgroup based LAN. Few or none of the clients need access to all local services. Rather they tend to be discrete groups of clients each using a different service.

For low bandwidth services this could be optimized by shared media workgroups and switching between the respective workgroups. Care will be needed in grouping on a physical/logical basis the clients with their appropriate services. Low bandwidth services may allow shared media within a workgroup to be filtered from other workgroups so that contention for bandwidth occurs mainly within each workgroup.

Medium bandwidth services may require switched connections to the services, but only the same shared media clusters for the clients. (The groups of clients should still be filtered from each other.)

4) Lattice-like clusters of high bandwidth services

This is a scenario in which all networked devices provide high bandwidth services used by all other devices. Optimization to each device in this scenario is imperative. High bandwidth connections, e.g. switched duplexed 100Mbps connections, should be provided to each device.

Note, that for low numbers of clients and local services the "stackable" class of network switches or switch is acceptable. For medium and high numbers "modular chassis" devices are a must.

**Common Switches Specifications**

Multi-port twisted pair switches allow several point-to-point segments to be joined into one network in a star-like configuration. Each workstation can potentially communicate with any other workstation connected to the same switches. One end of the point-to-point link is attached to a port on the switches and the other is attached to a network interface card in a workstation. If the switches is also attached to a backbone (larger network), then all workstations at the end of the twisted pair segments can communicate with any device connected to the same backbone (e.g., on another switches).

Troubleshooting connectivity problems is enhanced by devices organized in star configurations in two ways:

- Individual nodes can be easily isolated from other nodes
- Suspect switches can be quickly removed from a network backbone

The following is a description of the common specifications for both shared and switched Ethernet switches.

- **SNMP Management** - All shared and switched media switches must **minimally** implement Simple Network Management Protocol (SNMP) agent software. The SNMP agent in the switches communicates management information to an SNMP management software package running on a dedicated workstation. (The workstation typically requires 64 to 128 MB of memory, a 1 GB hard disk, a 133 Mhz processor, and runs either Unix, Windows 95 or Windows NT operating systems.) SNMP agents running in the switches must **minimally** support the Management Information Base (MIB) specification.

Stackable or chassis switches should also have enough management intelligence built-in so that a single node malfunction (e.g., excessive collisions, malformed frames, etc.) will result in auto-partitioning (turning off) of that node's switches port. This will effectively limit the impact of any single malfunctioning node disrupting the entire network. Setting up port thresholds to activate auto-partitioning requires proprietary MIBs (also called enterprise or private MIBs) which can best be manipulated by the vendor's SNMP management packages.

Some form of out-of-band management (typically modems connected through console ports) is mandatory. Out-of-band management that supports dialup TCP/IP (PPP) connections are desirable but not mandatory.

- **RMON Management** - As networks grow, the need to monitor the health of the network becomes essential. The Remote Network Monitoring (RMON) MIB specification allows an RMON probe (or agent) to gather information about the local network and deliver it to a management station that can process the information. An Ethernet switch should support the first four groups of RMON on a per port basis

**Shared Ethernet Switches Specifications**

Shared Ethernet switches are devices which connect multiple network devices to the same physical network media (cable). Shared switches function as "repeaters" because they take any incoming signal and repeat it out all ports. It is important to keep in mind that a repeater will only "clean up" and reshape signals crossing it; it cannot bridge or route network traffic because it operates solely at the physical layer (first logical layer of the OSI model).

The concept of **shared** access is related to the fact that all devices attached to the switches are contending for transmission of data onto a single network (i.e., a collision domain). This means that individual devices on a shared network will each only get a percentage of the available network bandwidth.

**Switched Ethernet Switches Specifications**

Unlike a shared media switches in which devices connected to its ports must contend for available bandwidth, a switched switches provides the full bandwidth (typically 10 /100/ 1000 Mbps) to each of its ports. The following is a presentation of the issues associated with switched Ethernet implementations:

- **SNMP Management**
- **Per Port RMON**
- **Port Mirroring**
- **Spanning Tree**
- **MAC Address Table**
- **ASIC Switching**
- ***(*No) Back Pressure.**
- **Buffering**

**General Switching Technology guidelines**

Switching Technologies shall be secure, in accordance with applicable IT security standards, and used to achieve LAN network device connectivity in Open Systems Interconnection (OSI) Layers 2, 3, and 4. Switching devices shall comply with IEEE 802.1p/Q standards and IETF Multi-Protocol Label Switching (MPLS) to provide scalable, interoperable, IP quality of service (QoS).

- Switching enhances security and network management. It improves network performance by enabling the balancing of network traffic across multiple segments at wire-speed, thus reducing resource contention, providing for scalability, and increasing throughput capacity.
- QoS features provide improved and more predictable network services by setting traffic priorities starting with the type of service (ToS) bits at Layer 2, then providing network traffic shaping, improved management, and congestion avoidance at Layer 3 with class of service (CoS) categorization. Applying QoS globally within a network infrastructure reduces packet loss and improves performance characteristics.
- IP QoS enables networks to support existing and emerging multimedia service/application requirements. It enables application-aware networking, in which a network services its packets based on application information within the packet headers. IP QoS provides end-to-end service and policy-based control of a private and/or public IP network’s performance.

- IEEE 802.1p enables network traffic prioritization and the seamless integration of data, voice, and video into converged services.
- IEEE 802.1Q trunking support enables segmentation of individual data, voice, and video client platform devices into separate logical virtual networks (VLANs). IEEE 802.1Q VLAN tagging uniquely identifies traffic from each VLAN, enabling traffic from multiple VLANs to share the same physical switch port link.

**Guidelines for Routing Technologies**

Routing Technologies shall be open, industry-standards-based for Internet and inter-network connectivity. Routing technologies should include the most currently approved versions of Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Routing Information Protocol (RIP), Integrated Intermediate System-to-Intermediate System (IS-IS), etc., and applicable multicast protocols including Internet Group Management Protocol (IGMP), Protocol Independent Multicast (PIM), Multiprotocol BGP (MBGP), etc. To avoid proprietary, single-source solutions, and vendor-specific extensions to open, industry-standard, routing protocols used for budget unit inter-network connectivity shall be generally available for use and implementation by third-party manufacturers. Vendor-specific extensions should also be in planned draft or draft form submittal to the appropriate standards approval body.

- Routing protocols provide the information needed to quickly and efficiently direct incoming IP traffic to the correct destination.
- Routing technologies operate over a reliable transport protocol (TCP).
- Extensions to standards-based routing protocols provide for both IPv6 and IPv4.

### 1.2 Guidelines for horizontal expansion of network

Following are the guidelines that can be referred to for horizontal expansion of network for small and large networks.

Small networks

If the network is small, one can always connect two hubs or switches together. This can be done in one of the following two ways:

1) By using a crossover cable to connect a "Normal" port on one hub to a "Normal" port on the other.
2) By using a regular UTP (Unshielded Twisted Pair) cable to connect the "Uplink" port on one hub to a "Normal" port on the other.

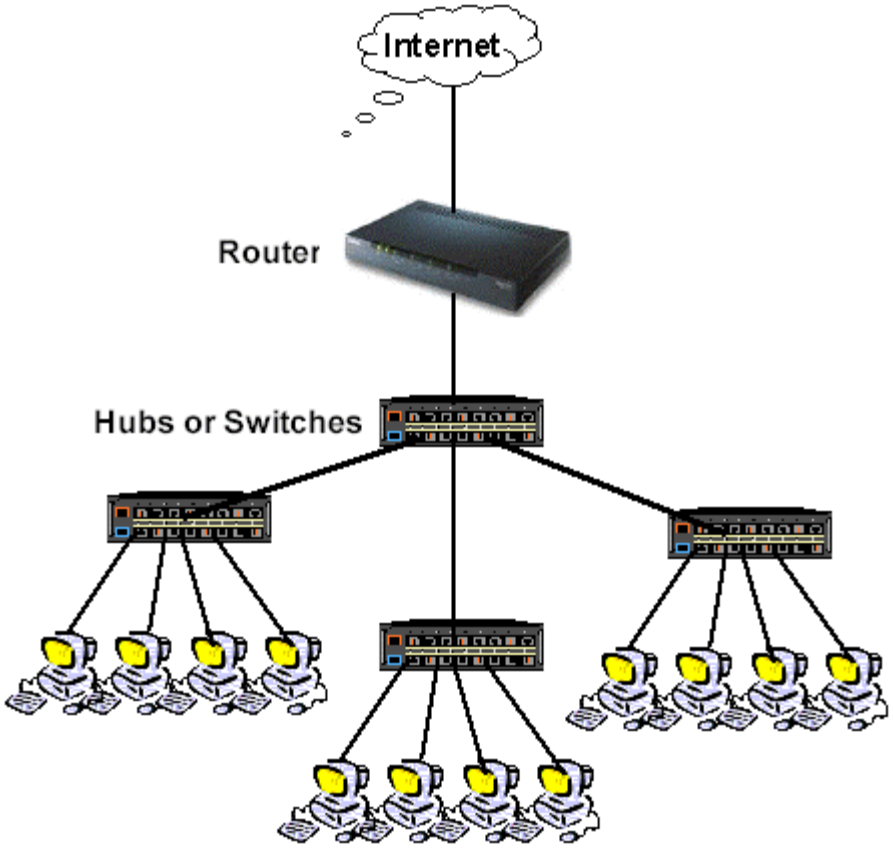
Note:

A port on a hub or switch is considered to be "Normal" unless otherwise marked. Some hubs and switches have a switch next to a port that controls whether it's a normal or uplink port. Others have two connectors on one port circuit. The "Uplink" connector has the connections for the Receive and Transmit wire pairs reversed from the "Normal" connector's wiring (just like using a "crossover" cable). The "Uplink" allows you to use a normal UTP cable to connect two hubs/switches together.

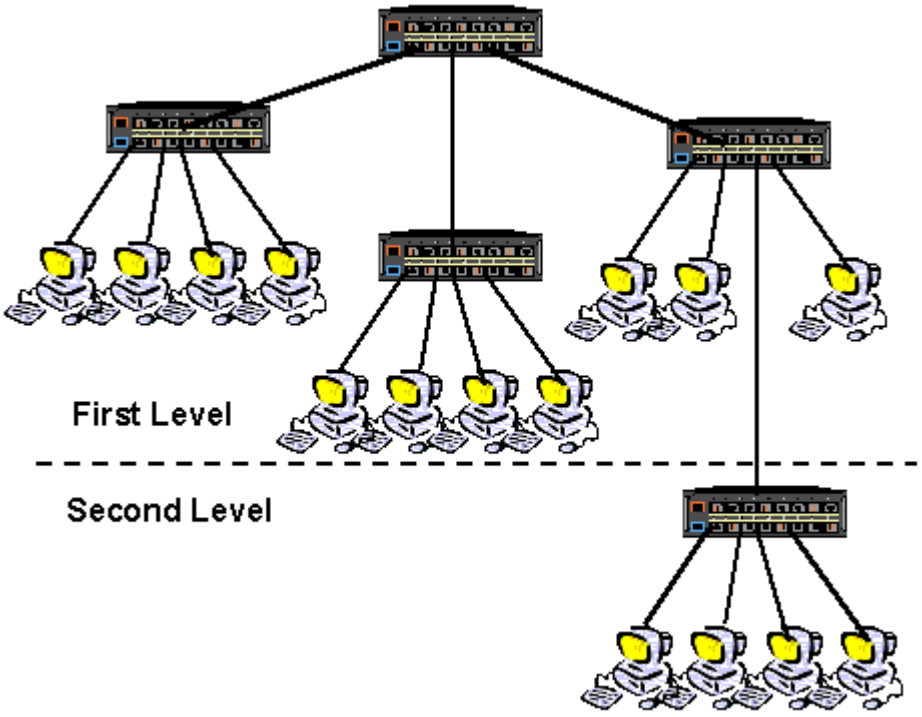
**Don't** connect cables in both the "Uplink" and the port connector next to it at the same time.

Larger networks

If the network is larger than two hubs can handle, a different method needs to be employed. The easiest thing to do is to take one hub and plug each expansion hub or switch into it, creating a "star" configuration of hubs. The diagram below shows such a configuration, connected to a router.



One can repeat the "star" to one more level as shown below.




**Don't** go to three levels or more as the network may experience the following problems

- Speed degradation
- Corruption of data packets and/or
- Functionality problems with the resulting network.

If even more ports are required, one may want to use a "stackable" hub or switch. "Stackable" hubs have a special connector on them that allow the **internal** circuitry to be connected together via a special cable. By connecting together the internal circuitry, the stacked hubs act as one hub with a lot of ports, instead of smaller hubs connected together.

### 1.3 Guidelines for integrating unmanaged switches

During upgradtion of networks that are significantly old or where cost was an important factor during the design, one would inevitably come across unmanaged network switches. An unmanaged switch simply allows Ethernet devices to communicate with one another. For example, when the Ethernet devices are connected (PC, network printer, and so on) to an unmanaged switch, they communicate with each other automatically.

The unmanaged switches use a protocol called "auto-negotiation" to agree upon certain communication parameters. One parameter they negotiate is the data rate — generally 10, 100 or 1000 MBps. Another is whether to use half-duplex or full-duplex mode. Thus as can be seen, it is difficult to have a port level control using an unmanaged switch. The following features would not be possible using unmanaged switches

- Blocking a particular port
- Setting speed limit on ports
- Prioritization of ports etc.

Upon expansion of a LAN space, it would be required to integrate these unmanaged switches with the managed switches. The following guidelines would help in making effective use of the unmanaged switches in tandem with the managed ones.

**1. Do not stagger unmanaged switches**

During horizontal expansion of network, it is advised that the unmanaged switches are not staggered, i.e. the unmanaged switches may not be connected to another unmanaged switch for horizontal expansion of network (as shown in figure 1)

**2. Let the unmanaged switches connect upward through managed switches or Routers.**

For upward connectivity, it is recommended that the unmanaged switches be connected to managed switches or to routers. An illustration of the same can be found in the figure 2 where the unmanaged switches are connected to ports in routers instead of being connected amongst themselves. This is a means to efficiently resolve problems by pinpointing the problem area at the switch level.

**3. Components that serve multiple equipment should be connected to a managed switch /router and not be connected to an unmanaged switch.**

Examples of such components would be application servers, database servers, web servers, wireless access points etc. These are components that serve a group of PCs, printers etc. It is thus advised that such components be connected to the managed switches or to the routers directly. This helps in quicker fault location, identification and resolution.

For instance, if one of the servers that is connected to an unmanaged switch goes down due to any reason, it becomes increasingly difficult to identify the server at the port level. But if the same server was connected to a managed switch, the same can be easily triangulated. This becomes increasingly important as the size of the network increases as along with the size, the complexity also increases.

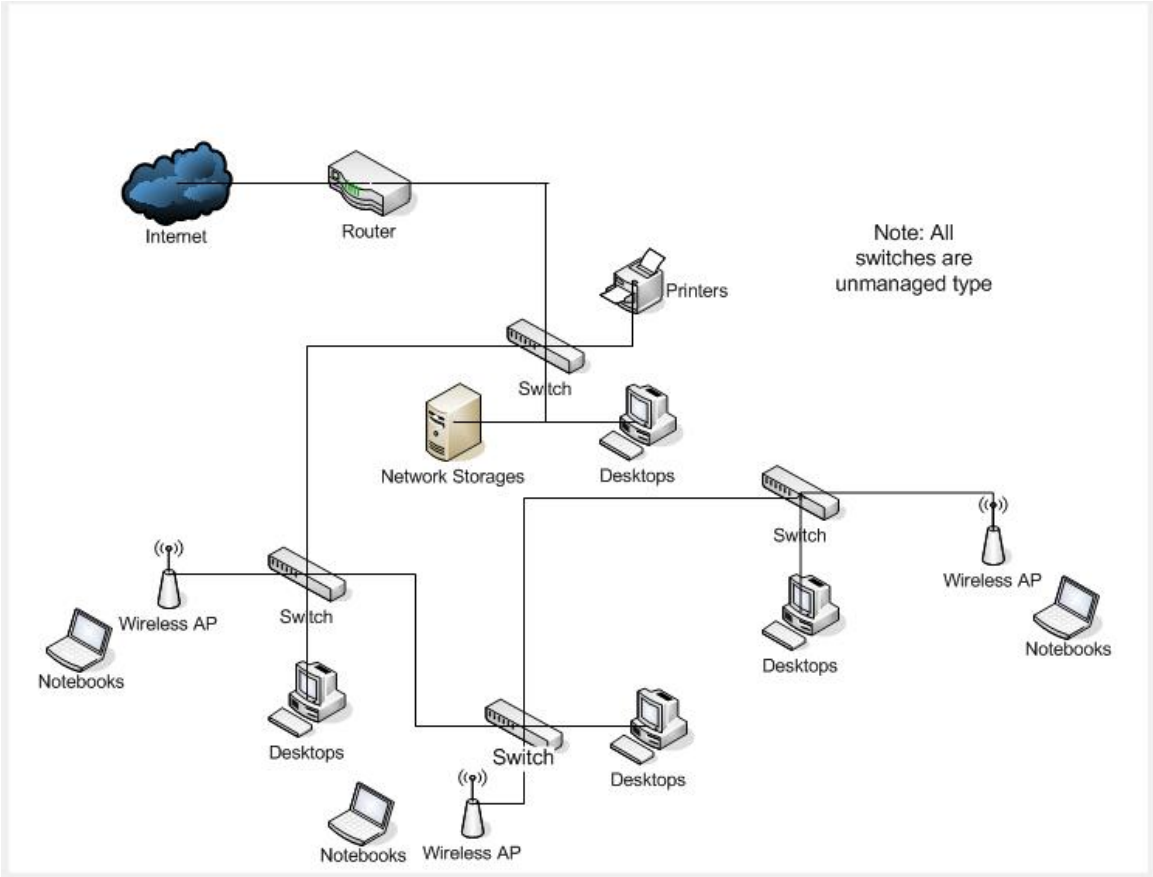



Figure 1 – Staggered Unmanaged Switches

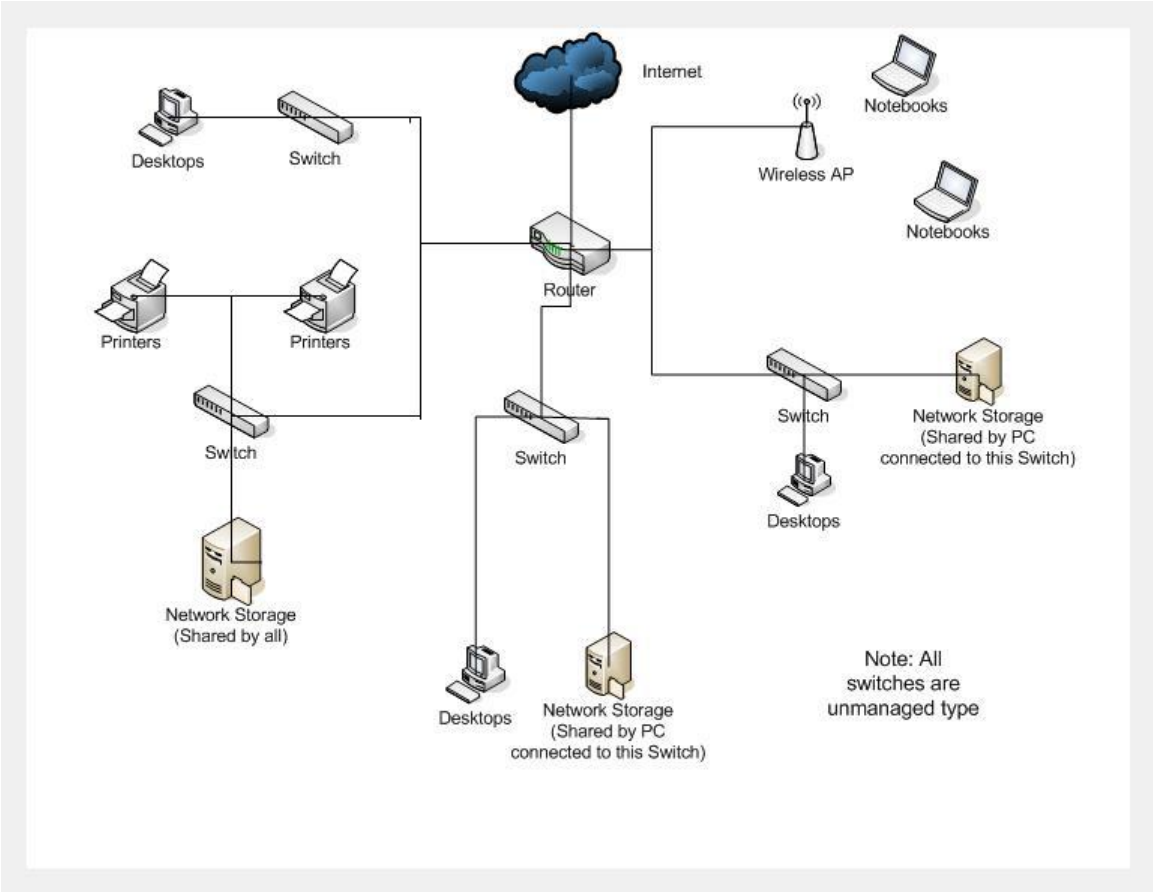



Figure 2 – unmanaged switches connected to managed switches

## 1.4 Guidelines for effective video conferencing

**Prior information to Network Administrator**

Video conferencing requires sufficient bandwidth to operate and thus tends to slowdown the network's performance. To avoid the degradation of network performance during video conferencing, it is advised that the network administrator be informed at least a day in advance. The network administrator can thus prepare the network by temporarily stopping low priority devices on the network. In doing this, the network administrator is releasing the bandwidth that is being occupied by these devices for the duration of the conference.

The information to the network administrator should contain at least the following

- Conference initiator details

- Number of participants and their details
- Date of conference
- Start time of conference
- Duration of conference

It is also advised that the conference initiator inform the network administrator as soon as the conference is concluded. Because, in the cases where the conference ends before the actual time, the low priority devices stay disconnected unnecessarily.

**Equipment**

It should be taken care that at least a minimum of the following equipment are available in the video-conferencing room to conduct efficient video conferencing

1. Video cameras - at least one at fixed wide-angle and another allowing focus and zoom control
2. Microphones with adequate sensitivity to pick up voice signals
3. Speakers
4. Monitors - small preview monitor along with a large monitor or wall-mounted projection screens.

Other common equipment might be a video player/recorder, a data sharing PC with a high-speed network connection.

**Use of relevant software**

The video conferencing software chosen should be an effective tool in conducting organized video conferencing amongst multiple participants from different offices. Thus care should be taken in the selection of the software. It should be made sure that the software has at least the following functionalities

1. Multi-Party Management – should be a secure web browser-based application that provides complete management of multi-party video communications systems and infrastructure devices.
2. Scheduler with Automatic Calling – the automatic calling scheduler would provide a hands-off, easy-to-use scheduling and call launch platform. The network administrators may simply discover and manage systems, inform the system of

appropriate associations between endpoints and infrastructure, then sit back and let the system handle everything from system scheduling to call establishment.

3. End user scheduling of conferences – the system should be capable of collecting the processing video conferencing requests from the end user. The system should automatically store this request in the queue and should later initiate the call and allocate video resources where they are needed.
4. Reporting – the system should have adequate graphical reporting capability. This shall help the network administrator in tracking usage, service level agreements and cost of ownership. The system should also be able to generated automatic scheduled reports and send across to the administrators in the various popular formats (like PDF, Xls etc). These reports should be delivered to their inboxes or to handheld devices as configured in the system.

**Annexure -5 - Network Components Do's & Don'ts**

### 1.1.1 Cable-Do's & Don'ts

- Although the maximum cable length for a Cat 5e/6/7 system is often reported to be 100m, this length is inclusive of patch and drop leads. Cable testers however, when set to perform a 'Basic Link' test, take this into account and you will find that the maximum length is set to either 90m or 94m depending on the standard you are testing to. Also, because the length is measured with a Cable Analyser it is not the physical length of the run but the copper length that is measured. The copper length is longer due to the twists in the cable pairs, so if a run looks like it might be over 85m it would be wise to check it before it is tied up and terminated.
- Each outlet cable should be run directly back to the patch cabinet that is one cable per outlet. A transition point or connection box is allowed if necessary, but in practice this can be more trouble than its worth.
- Care should be taken when pulling cables in to ensure that they are not kinked or nicked.
- Cable routes should be planned to avoid fluorescent light fittings and power cables (exceptions can be made in the case of optical fibre). They should not be run in the same conduit as power, or the same channel of a trunking system, and where they are run parallel to power they must be at least 60mm apart (BS7671-92) . Crossing power cables is allowed but it must be at right angles, and some form of bridge should be used.
- A means of supporting the cables should be installed such as cable tray, catenary wire or cable tie fixings, tying cables to ceiling hangers is not permitted. Cables should be tied at a minimum of 500mm intervals on horizontal runs and more frequently on vertical runs, with no more than 48 cables in a loom. Cable ties should only be finger tight to avoid crushing the cables as this could affect the cables performance characteristics. Do not use cable tie guns or staple guns.
- Cable trays should be used under false floors, if not, a suitable method of keeping the cable off the floor slab should be employed. This is because the lime in the concrete apparently reacts with the cables sheathing, and over time could damage the cable. I personally think the cable will have outlived its usefulness long before this could have any affect on the cables performance.

- Care should be taken when pulling cables into trunking to avoid damage due to snagging. Trunking partitions should be used to separate the data cables from power, and bridges should be used where data cables have to cross the mains.
- When terminating patch panels, cable looms should not exceed 48 cables. Each cable loom should then be tied in a tidy manner to a cable tray fitted the full length of the cabinet.
- All terminating should be carried out according to the manufacturers' instructions and guidelines, and the standards for generic cabling systems. The cable sheath should be stripped back no more than 13mm from the point of termination and the twist rates should be maintained.
- Cable ties MUST be fitted to the individual RJ45 modules in the patch panels and outlets to support each cable.
- When terminating outlets, care must be taken to avoid damaging the copper cores when stripping back the outer sheathing.
- Excessive amounts of cable should not be left in the outlet backbox. Care should be taken when attaching the outlet faceplate not to kink, trap or strain the cable.
- Cable tray should be fitted in cabinets housing structured cabling to keep cable looms secure and tidy, and to provide room for any additional cabling.
- All cabinets must be earthed to the 16th edition IEEE wiring regulations (British regulations). Where shielded cable is used the earth should be clean and where two cabinets are linked with a copper backbone (shielded or unshielded) a minimum of 10mm² earth wire should also be installed to cross bond the cabinets.

### 1.1.2 Fiber-Do's & Don'ts

**Pulling Fiber Optic Cable**

Pulling fiber optic cable isn't hard at all, since the manufacturer takes great pains to make sure the cable design protects the fibers during installation. Fiber cable can be pulled with much greater force than copper wire if you pull it correctly. Just remember these rules:

- **Do not pull on the fibers, pull on the strength members only :**

The cable manufacturer gives you the perfect solution to pulling the cables, they install special strength members, usually duPont Kevlar aramid yarn or a fiberglass rod to pull on. Use it! Any other method may put stress on the fibers and harm them. Most cables

cannot be pulled by the jacket. Do not pull on the jacket unless it is specifically approved by the cable manufacturer and you use an approved cable grip.

- **Do not exceed the maximum pulling load rating:**

On long runs, use proper lubricants and make sure they are compatible with the cable jacket. On really long runs, pull from the middle out to both ends. If possible, use an automated puller with tension control, but we've seen jobs done with a mule providing the pulling force.

- **Do not exceed the cable bend radius.**

Fiber is stronger than steel when you pull it straight, but it breaks easily when bent too tightly. If you put a kink in the cable, you will harm the fibers, maybe immediately, maybe not for a few years, but you will harm them and the cable must be removed and thrown away!

- **Do not twist the cable.**

Putting a twist in the cable can stress the fibers too. Always roll the cable off the spool instead of spinning it off the spool end. This will put a twist in the cable for every turn on the spool! If you are laying cable out for a long pull, use a "figure 8" on the ground to prevent twisting (the figure 8 puts a half twist in on one side of the 8 and takes it out on the other, preventing twists.) And always use a swivel pulling eye, because pulling tension will cause twisting forces on the cable.

Make sure the cable is long enough for the run. It's not easy or cheap to splice fiber and it needs special protection. Try to make it in one pull, possible up to about 2-3 miles.

### 1.1.3 Routers-Do's and Don'ts

- Do prevent address spoofing at the edge of a Organisations network. At minimum, routers at the edge of an organisation should block inbound traffic with source IP addresses claiming to be from internal networks. Similarly, the source IP address of any outbound packet should only be from an internal network.

- Do prevent bogus routes. Some IP addresses should never be seen on the Internet. These include not only the private addresses specified in RFC 1918 but also those networks designated as reserved by the Internet Assigned Numbers Authority (IANA). IANA-reserved routes, known as bogons, change over time, so it's a good idea to keep current on which networks to block. One good source is the bogon-announce mailing list. Details, a filtering FAQ and links to other filtering information are available on the Web.
- Do block unwanted applications. An easy method for stopping unwanted traffic is simply to filter on the well-known protocol and/or port numbers that a given application uses. For example, a router could block outbound telnet sessions by dropping any packet with destination TCP Port 23. The major caveat with this technique is that it does not protect against rogue applications that change port numbers, for example by sending peer-to-peer traffic over Port 80 (which is reserved for Web traffic).
- Do track usage: How many times did users visit a given network? How much bandwidth did a given application consume? Most routers' filters can be set to answer these questions by logging the number of times a filter was invoked. In the case of Cisco's access lists, enabling logging is simple: Just append the word "log" at the end of the filtering conditions. Some other devices, such as those from Enterasys Networks and Tasman, automatically log by default.
- Do lighten the load. Packet filtering can impose several performance penalties on Cisco routers. One strategy that considerably reduces CPU utilization is to use routing instead of filtering. For example, it's possible to route traffic to or from unwanted addresses to the null 0 interface.
- Do pay attention to order. Routers process filters in order. For every packet that comes in, a router checks the packet against its first filter, its second filter and so on until it finds a match. If the first rule in an access control list (ACL) is to deny all traffic, the router won't forward any packets. It's a good practice to end an ACL with a deny-all filter, but be sure it's preceded by filters that explicitly allow traffic that should be permitted.
- Don't forget about routing. As soon as a single filter is invoked, many routers automatically will block traffic unless it is expressly permitted. A common error when configuring ACLs is to omit filters that permit routing traffic to pass.
- Don't use routers in place of firewalls. Packet filters block access, but that's where the similarities to firewalls end. As a network-layer device, a router can't track state

on transport- or application-layer sessions, both critical requirements of a firewall. Packet filtering offers some security (and it's certainly better than nothing), but it won't prevent an attacker from mounting many attacks a firewall could stop.

**Annexure -6 List of Logs**

| Source | Type of log | Log ID | Events logged | Criticality of Source | Log Rotation Frequency | Retention Period | Review Frequency | Criticality of log |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

### 1.1 Annexure 2 – Log Analysis Report

| Log ID | Period | Review Date and Time | Reviewed By | Analysis Results | Action Initiated (if any) |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

## 1.2 Annexure 3 – Consolidated Log Report

| Source | Type of log | Log ID | Period | Review Date and Time | Analysis Results | Action Initiated | Comments |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

**Annexure-7**

**SPECIFICATIONS OF NEW EQUIPMENTS**

## 1. CABLE LAYING WORKS

### 1.1 General

The Underground OFC / Copper Cables are extensively used in outdoor network of GSWAN / SCAN / SICN networks. The cables are laid from GSWAN / SICN nodes or from SICN RUs (Remote Units) to Distribution Points (DPs). For the purpose of flexibility, Pillars / Junction boxes are introduced in the network. The primary cables, which are of higher size, are laid from GSWAN / SCAN / SICN locations to Pillars / Junction boxes. The distribution cables are laid from Pillar / Junction box to DP. The capacity of Pillars and DPs are decided in accordance with demand and size of the net work. The quality of construction of U/G cable Net Work decides the quality and reliability of GSWAN / SCAN / SICN services, delivered to the users to a large extent. Therefore, the construction practices of the U/G cables should be of very high quality, strictly in accordance with constructions specifications.

The Cables / Components / Accessories to be used in the project must be of specified brand and wherever it is not specified it must be of standard quality (ISI / BIS standards) and must be approved by BSNL / Railtel/ Defense / GAIL/ Power Grid Corp. Bidders have to supply the cables of any of these brands: Finolex, Delton, RPG, Birla Ericson, Sterlite, D –Link, DAX. Vendor will have to provide test certificate from the manufacturer, to ensure the quality of the each and every lot of the cable / material used. The bidders have to supply the HDPE pipe of any of these brands: Parixit, Dultron, and Finolex. Bidder will also have to obtain a quality certification from EQDC, Gandhinagar, for the all the passive material such as Cables, accessories, GI / HDPE pipes, Cable guides, Casing & Capping, Patch Cords, Racks, DP, Krone / connectors etc., used for the work. Vendor will have to bear the cost for all such testing and GoG will not reimburse the same.

### 1.2 The Works Involved:

The Under Ground Cables are buried to a depth such that the top of the cable is One meter (100 Cms.) below the normal ground level. The items of work involved in U/G Cable laying are as under:-

1) Excavations of trench up to a depth such that the top of the cable is 1 meter below the normal ground level according to the construction specifications.

2) Laying and pulling of cables in trenches are through pipes/ ducts.

3) Placing of Half round RCC Pipes / Stones slabs /Pre cast RCC Slabs /Layer of Bricks as per specifications.

4) Back filling in compacting of the excavated trenches according to the constructions specifications and removal of excess earth from the site.

5) Construction of pillar foundations erection, painting and sign writing of pillars.

6) Erection, termination, painting and sign writing of DPs

7) Termination of Cables in MDF & Pillars.

8) Jointing and End-to-End testing of Cables – Correspondence and Electrical tests. Supply, fixing, painting and sign writing of root and joint indicators and Documentation.

### 1.3 Construction Specifications:

**Classification of Soil**: For the purpose of trenching, the soil shall be categorized as under.

**Soft Soil:** This will include all types of soils- soft soil/hard soil / morrum i.e. any strata, such as sand, gravel, loam, clay, black cotton morrum, single, river or nalla bed boulders, soiling of roads, paths, densely pebbles/stones etc., lime concrete, mud concrete and their mixtures which for excavation yields to the application of picks, showels, sacrifiers, ripper and other manual digging implements including chiseling.

### 1.4 Footpaths / Along Road Side:

1) Trenching on Foot Path or along Road on carpeted surface may be necessary in certain stretches where roads have been metalled edge to edge and there is no un-metalled corridor or footpath available for trenching and laying the cables.

2) Tarmac (Asphalt) Foot Path / Road: means Footpath / Road with tarmac surface with or without compacted strata below the tarmac surface, irrespective of thickness of Tarmac/Metal.

3) Kharanja: means Footpath / Road covered with various types of bricks with or without compacted strata below the surface, irrespective of thickness of bricks.

4) Tiled Foot Path / Roads**:** means Footpath / Road covered with various types of tiles/stone slabs with or with out compacted strata below the tiled surface, irrespective of thickness of tiles / stone slabs.

5) Cement Concrete Foot Path Road: means the surface on Footpath / Road covered with CC (Cement Concrete) with or without compacted strata below the surface, irrespective of thickness of cement concrete.

### 1.5 Road Crossings:

1) "Tarmac Or Asphalt Road" means the road surface, which is metalled by sphalt/tarmac normally having compacted strata below the metalled surface, irrespective of thickness of asphalt/tarmac.

2) Kharanja Road: means road covered with various types of bricks with or without compacted strata below the tiled road surface, irrespective of thickness of bricks.

3) Tiled/CC Road: means road made of tiles of any type/stone slabs/bricks or CC road normally having compacted strata below the tiled/CC surface, irrespective of thickness of tiles/CC.

4) RCC Road: means the surface made of cement concrete duly reinforced with steel bars normally having compacted strata below RCC, irrespective of thickness of RCC.

5) WBM road: means water bound mecadam surface made of stone, metal and gravel and rolled with road roller.

6) At road crossings, the trenches shall be so dug that top of RCC pipe shall be at one meter depth from ground level.

### 1.6 Excavation of Trenches

Before excavation of trenches, the route should be marked for trenching. Care should be taken to see that the route of the trench to excavate is reasonably straight avoiding the existing underground service.

The Vendor should take trial pits to locate the underground services before commencement of actual trenching. These trial pits shall be 30 cms. wide, 120 cms. deep and 120 cms. long at right angles to the proposed trench at an interval of 20 to 50 Mtrs along the proposed cable route. If a slab is encountered, the same may be removed and trial pits may be made.

In city areas, the trench will normally follow the footpath or the road except where it may have to come to the edge of carriageway or cutting across roads with the specific permission from the concerned authorities maintaining the road, (such permission shall be obtained by the Vendor). Outside the city limits, the trench will normally follow the boundary of the roadside land. However, where the roadside land is full of burrow pits or when the cables have to cross culverts / bridges or streams, the trench may come closer to the road edge or in some cases, over the embankment or shoulder of the road (Permission for such deviations for cutting the embankment as well as shoulder of the roads shall be obtained by the Vendor).

The alignment of the trench will be decided by Engineer-In-Charge or by TCIL. Once the alignment is marked, no deviation from the alignment is permissible except with the approval of Engineer-In-Charge or TCIL. While marking the alignment only the centre line will be marked and the Vendor shall set out all other works to ensure that, the excavated trench is as straight as possible. The Vendor shall provide all necessary assistance and labour, at his own cost for marking the alignment. Vendor shall remove all bushes, undergrowth, stumps, rocks and other obstacles to facilitate marking the centre line without any extra charges. It is to be ensured that minimum amount of bushes, shrubs shall be removed to clear the way, and the Vendor shall give all consideration to the preservation of the trees.

The line-up of the trench must be such that cables shall be laid in a straight line except at locations where it has to necessarily take a bend because of change in the alignment or gradient of the trench.

### 1.7 Methods of Excavation:

In city limits as well as in built up areas, the Vendor shall resort to use of manual labour only to ensure that no damage is caused to any underground or surface installations belonging to other public utility services and / or private parties.

However, along the Highways and across country routes, there shall be no objection to the Vendor resorting to mechanical means of excavation, provided that no underground Installations exist in the path of excavation, if any, are damaged.

There shall be no objection to resort to horizontal boring to bore a hole of required size and to push through G.I. Pipe through horizontal bore at road crossing or rail crossing or small hillocks etc.

Necessary barricades, night lamps, warning boards and required watchman shall be provide by the Vendor to prevent any accident to pedestrians or vehicles.

When trenches are excavated in slopes, uneven ground, inclined portion, and the lower edge shall be treated as normal level of the ground for the purpose of measurement of depth of the trench.

In certain locations, such as uneven ground, hilly areas and all other places, due to any reason whatsoever it can be ordered to excavate beyond standard depth of 100 Cms. above the cable to keep the bed of the trench as smooth as possible.

If excavation is not possible to the minimum depth of 100 Cms. above the cable, as detailed above, full facts shall be brought to the notice of the Engineer-In- Charge / TCIL in writing giving details of location and reason for not being able to excavate that particular portion. Approval may be granted in writing under genuine circumstances.

The Vendor shall be responsible for all necessary arrangements to remove or pump out water from trench. The Vendor should survey the soil conditions encountered in the section and make his own assessment about dewatering arrangements that may be necessary. Wherever the soil is hard due to dry weather conditions, if watering is to be done for wetting the soil to make it loose, the same will be done by the Vendor.

**1.8 Trenching near culverts / Bridges:**

At bridges and culverts, the cable shall be laid in GI pipe of suitable size with the permission of concerned authorities maintaining the roads/bridges. The Vendor shall obtain such permission. While carrying out the work on bridges and culverts, adequate arrangement for cautioning the traffic by way of caution boards during daytime and danger lights at night shall be provided.

The GI pipe should be clamped to the outside of the parapet wall of the culvert or bridge with the help of clamps, nails, nuts, bolts and screws of suitable size to ensure that the pipe is securely fixed. The GI clamps should be of minimum 25 mm width and 3 mm thickness and should be fixed at an interval of 50 cms. If necessary, the pipe should be taken to the parapet walls at the ends where the wall diverges away from the roads. The work should be carried out in consultation with the authorities concerned maintaining the roads and bridges.

In case of small bridges and culverts, where there is a likelihood of their subsequent expansion and remodeling, the cable should be laid with some curve on both sides of the culvert or the bridge to make some extra length available for readjustment of the cable at the time of reconstruction of culvert or the bridge.

**1.9 Excavation in Surfaced Strata:**

**Excavation on Footpath:** The excavation of trenches in all types of footpaths including dismantling of asphalt/all type of tiles/CC and WBM shall be done up to a depth such that the top of the cable is 1.0 M below the normal ground level. The excavation on the footpaths will be done manually. The Vendor shall have to provide shoring wherever necessary, in case the depth of trench is more than one meter. It is expected that the other services may be present below the footpath, therefore, extra care need to be exercised while excavation of trenches.

**Excavation of Trenches along the roads (which are carpeted end to end):** The excavation of trenches along the roads, which are, carpeted from end to end including dismantling of' asphalt, concrete and WBM shall be done up to a depth such that the top of the cable is 1.0 M below the normal ground level. The excavation along the roads shall be done manually. The Vendor shall have to provide shoring wherever necessary, in case the depth of trench is more than one meter. It is expected that the other services may be present below the roads, therefore, extra care need to be exercised while excavation of trenches.

### 1.10 Excavation at Road Crossings:

The excavation of trenches in all types of roads including dismantling of asphalt / all type of tiles / CC and WBM shall be done up to a depth such that the top of the RCC pipe Is 1.0 meter below the normal ground level. After excavation of trench, RCC Pipes of 100mm/ 150mm/225mm /300mm dia shall be laid at the road crossings. The roads, which are broad, may be opened for half their width, allowing the other half for use of vehicular traffic. The second half of the width should be opened after laying pipes and reinstating the first half of the trench. Pipes laid in the second half should be coupled firmly with those laid in the first half. Care must be taken to couple the pipes fully. The pipes should be laid with a slight slope from the center to the sides of the road to prevent collection of water. 8 mm PP Rope shall be drawn through the laid pipes to facilitate cleaning and cable pulling at a later date before closing the trench.

As the work on road crossings entails lot of inconvenience to vehicular traffic and pedestrians, it is desirable to bury extra pipes for future expansion at the initial stage itself. The spare pipes must be sealed properly at both the ends of the road to obviate the possibility of pipe getting chocked due to settlement of sedimentation etc. The Vendor shall have to provide shoring, wherever necessary, in case the depth of trench is more than one meter. Necessary barricades, night lamps, warning boards and required watchman shall be provided by the Vendor to prevent any accident to pedestrians or vehicles.

### 1.11 Trenches of Less Depth:

The depth of trench is very important for future life of cables. Therefore, it is very much necessary for Vendor to ensure that the standard depth is maintained in normal circumstances. However, due to obstructions, if the standard depth cannot be achieved, lower depths up to certain limits are acceptable by the authorities with extra protection as per specifications. The relaxation shall be obtained from the Engineering In charge / TCIL, giving reasons for not achieving standard depth.

### 1.12 Laying of Cables:

After excavation of trenches, approximately 5 Cms thick bed of soft soil/ or sand (in case the excavated material contains sharp pieces of rock/stones) is laid before directly laying the cable. Adequate care shall be exercised while laying the cables so that the cables are not put to undue tension/pressure as this may adversely affect the electrical characteristics of cables with passage of time.

Sharp bends shall be avoided. Bends, if any, the radius of curvature should be more than at least six times the diameter of the cable. After the completion of laying, sand/ sieved earth, free of stones etc., shall be placed over the cable to a height of 7.5 Cms. duly levelled and rammed lightly to form a bedding for warning bricks or Half round RCC pipes/ stone slab/ Pre cast RCC slab for mechanical protection.

The cables may be required to be pulled through RCC/ GI Pipes at road crossings, Extra care should be taken to avoid damage to the cable while pulling through pipes, which may occur due to kinks. The Vendor should have the required tools and equipments for the purpose to complete the job in a professional manner.

The Vendor shall ensure that trenching and cable laying activities are continuous, without leaving patches or portions incomplete in between.

When there are number of cables of the same size in the same trench, it becomes difficult to identify the particular cable at time of maintenance. Therefore, identification collars bearing L.I. Number of the cable shall be tagged to all the cables. The identification collars shall be provided at an interval of not more than 2 meters.

### 1.13 Placing of Half Round RCC Pipes / Layer of Bricks

After laying of cables, it is covered by a consolidated layer of 8 Cms. of soft earth (or sand in special cases where excavated material contains sharp stones/objects) which should be free from stones or other sharp objects, carefully pressed and lightly tamped. On this layer of soft earth, a layer of half round RCC pipes (100/150 mm dia) / Bricks is placed as a warning layer and also as a mechanical protection. The choice for protection layer out of half round RCC Pipes or bricks may be decided based on availability and comparative cost.

### 1.14 Back Filling and Compacting of the Excavated Trenches:

After laying the cables and providing warning/protection layer as per specifications, the remaining portion of the trench shall be filled in and well tamped in steps. The trench should be back filled in layers not exceeding 20 cms. Each at a time and rammed. The Vendor shall remove the excess earth from the site and leave only a crown of earth rising approximately 5 cms. in the centre. This allows for natural subsidence. When digging on footpaths, along roads and crossings, care should be taken to see that the road is made motorable as soon as the work is completed. The local authorities shall do the permanent reinstatement of roads and pavement.

### 1.15 Erection of Pillars:

The pillars should be installed in safe places on footpaths at suitable locations convenient and accessible for maintenance. The positions close to the edge of footpaths, near transformers or below Electric Lines particularly H.T. Lines must be avoided. The location of pillar, which may obstruct the view of drivers of vehicles as on kerb lines at street

intersections, locations in which the doors of the pillars when opened constitute a danger to pedestrians or traffic must be avoided. In general, the pillar shall be so located that reasonable and safe working conditions to the staff are possible throughout the year. The height of the pillar shall be such that the pillar does not get submerged during rains.

**1.16 Erection of DPs:**

The Distribution Points (DPs) are fitted on poles, walls or in the staircase walls easily accessible for maintenance, to terminate distribution cables coming from pillars. The items of work in erection of DPs are as under:

1) Fixing of 20/32 mm G.I.Pipe with the help of clamps, nails and saddles at every 30 cms. The clamps should be made of 25 mm wide and 3 mm thick, G.I. strips properly galvanized.

2) Pulling of L.I. Cable (5 Pairs/10 pairs/20 pairs/50 pairs) through 20/32 mm dia G. I. Pipe of approximately 7 to 10 ft. and terminating the cable pairs in DP box and fixing of DP box on the wall with the help of suitable rawl plugs/wooden gitti and screws.

**1.17 Termination of Cables in MDF & Pillars:**

The U.G.Cables is terminated on tag blocks on line side of the MDF. The MDF consists of iron framework and line side tag blocks are fitted on verticals. In the department, depending upon the height of the MDF room, MDFs of different sizes are erected. For simplicity and uniformity, a standard numbering scheme of verticals, tag blocks and tag numbers in the tag block is followed.

While terminating the cables in MDFs and Pillars, the correspondence of pairs shall be maintained from the point of view of counting of pairs and maintenance of the cables. In case of armoured cables, the armour of the cable shall be connected to the C.T box-mounting frame in the pillar and to the verticals of MDF, which are earthed.

The work of ‘‘termination on MDF and pillars ‘‘includes

1) Fixing of tag blocks on MDF vertical/CT boxes in Pillars.

2) Drawing the cable in to the pillar and removing the cable sheath for required length.

3) Providing earth continuity with the armour of the cable(s).

4) Cleaning the insulated conductor and covering the formed bunches with PVC sleeve/tape.

5) Termination of cable pairs in Tag blocks/CT boxes.

6) Sign writing with white enamel paint of reputed brand on inner panel of the pillar shall be done indicating the termination details. On MDF, the written labels shall be put in place provided for it indicating the termination details. The Engineer-in-charge shall give the details of sign writing.

7) The termination of cables should be done using standard tools.

### 1.18 Jointing of cables:

The quality of jointing work is of immense importance and therefore, the jointing work should be done experienced jointers using standard tools and accessories.

The work of cable jointing involves jointing of pairs by twisting. The quality of joint is vital for overall electrical characteristics and quality of transmission of the subscriber loop and therefore, the same has to be done meticulously.

The items of work involved in jointing are as under:

1) Digging the Pit for the Joint.

2) Preparation of cable ends for jointing.

3) Jointing of cable conductors by twisting or by machine jointing using modular connectors.

4) Closing the joint & Flooding of the joint (Flooding of Joints shall be mandatory).

5) Providing protection to the joint with half round RCC Pipe/ Briks

6) Back filling and compacting.

7) Providing joint indicator and noting distances from three permanent points for future reference to locate the joints.

The Vendor shall make hundred percent pairs available from end to end. To ensure the availability of 100% pairs end to end it is a good practice not to close the joints until all the pairs are tested from MDF to pillar for primary cable work and from pillar to DP for distribution cable work. In case of some pairs missing, the defects should be rectified at this stage it self, as the joints are still kept open. Once, all the pairs are available, joint shall be closed properly using jelly and other accessories as per instructions. Proper and adequate filling of jelly in the joints is of importance as any water ingress and trapped in the cavities will result into low insulation fault at later date.

### 1.19 End-to-End Testing:

The cables are to be tested for continuity of pairs and electrical and transmission characteristics of the cable pairs, between MDF and pillar in case of primary cables and pillar and DPs in case of distribution cables separately. Broadly, the following Parameters are tested

1) Insulation
2) Cross Insulation
3) Continuity
4) Loop resistance
5) Transmission loss
6) Cross talk level.

### 1.20 Cable route & Joint Indicators:

Cable route and joint indicators are to be provided to indicate the cable route and location joints. The route and joint indicators are to be used for cables laid in rural areas, as availability of landmarks over wide expanse of lands is scanty. The route indicators are to be placed at every 200 mts. and at every place where the cable changes direction. Joint indicators are to be provided at all joints. For the sake of uniformity and from viewpoint of identification of cable at later date for maintenance, the route / joint indicators shall be provided in the alignment of the trench.

The route/Joint indicators shall be painted with Primer before painting with oil paint. The route indicators shall be painted with yellow paint and joint indicators shall be painted with red paint.

**1.21 Documentation:**

The documentation, consisting of route diagrams, depicting joint locations, termination details of cables on MDF, pillars and D.Ps. is of immense help at the time of maintenance or undertaking any re-arrangement work.

The documentation shall be prepared primary cable wise for one or more than one primary cables with all its pillars shown and for all its pillars the distribution cables shown pillar wise, for the each work order. Vender will have to undertake preparation of route diagram depicting alignment of cables on roadsides on a geographical map. Though it is desirable to prep are these diagrams on geographical maps to the scale but in case geographical maps are not available, the maps should be constructed to a reasonable accuracy by taking details from the local bodies of the area. On this diagram, besides showing alignment of the cable, the topographical details of the road, location of pillars and landmarks along side should also be shown to locate the cable(s) easily as and when required.

**2. <u>FOR LAN WORKS</u>**

The Cables / Components / Accessories to be used in the project must be of specified brand and should have been consumed by BSNL/Railtel /Defense / GAIL/ Power Grid Corp.

**2.1 For OFC and JFC:**
The specified brands are Finolex, Delton, RPG, Birla Ericson, Sterlite, D-Link, DigiLink, Molex, and DAX.

**2.2 For the CAT-5 / CAT-6 cables:**
The specified brands are DAX, DLINK, HCL, DigiLink, Finolex, D-Link and Molex.

**2.3 For the Passive Networking Components:**
The specified brands are Systimex, AMP, D-Link, Molex, DAX, HCL, 3Com, DigiLink.

**2.4 For Casing Capping:**
The specified brands are Modi/ Precision/ Presto Plast/ Vraj etc.

**2.5 For Race Way:**
The specified brands are Precision/ Presto Plast/ Vraj/ Plasto etc.

**2.6 For Flexible PVC Pipe:**

The specified brands are Precision/ Vraj & Presto Plast, Duraflex

**2.7 For Rigid PVC Pipe:**

The specified brands are Finolex & Deltron, Precision, Vraj

**2.7 For Racks:**

The specified brands are Spider/ Alpine/ APW/ Valrack

**2.8 For HDPE pipe:**

The specified brands are Parixit, Dultron, and Finolex.

Vendor will have to provide test certificate (ETL / UL etc.) for the cable / material used, to ensure the quality of the each and every lot.

All work performed on this project will be installed in accordance with the current edition of the following:

1) BICSI Telecommunications Distribution Methods Manual
2) BICSI Cabling Installation Manual
3) ANSI/TIA/EIA Standards
4) All local codes and ordinances.

During the installation activities, records and route layout diagram must be kept of all items installed, including reference to cable pathways used, final location, identity of cables and equipment. The presentation of all of these records will provide the "As-Installed" basis for all future reference to the installation.

The Optical Fiber and UTP cabling shall be installed in accordance with manufacturer's installation instructions. The installer will ensure that the manufacturer's specifications for the Optical Fiber cable and the UTP cables meet the transmission characteristics required by Cabling Standards.

All installed cables, termination boxes, distribution panels and wall outlets shall be marked and numbered in accordance with Administration Standard for the Telecommunications Infrastructure.

The documentation required at the completion of the installation phases shall contain all of the following information, together with any other information the installer has acquired during the installation.

1) ''As-Installed'' documentation, showing total cabling and connections installed using floor space plans and cable record sheets. This documentation must show all cables and outlets incorporating the full numbering and marking convention supplied.

2) All test results and certification information, identified by cable, connection and numbering convention, necessary for all Optical Fiber and copper cables.

3) All the work carried out by the bidder need to be registered in the concord software (or any other Network Management software) used by DST/TCIL and enter data in centralized GIS mapping of GSWAN connectivity as per the requirement of DST.

## 3. LAST MILE EQUIPMENTS

### 3.1 Transceiver/Media Converter

| Transceiver / Media Converter | |
|---|---|
| **(A) Mini GBIC Transceiver Single Mode type for Manageable switch** | Small Form Factor Pluggable module – Mini GBIC 1000 based LX module t support Gigabit speeds over 9/125 Single mode Fiber up to a distance of 10kms |
| **(B) Mini GBIC Transceiver Multi Mode type for Manageable switch** | Small Form Factor Pluggable module – Mini GBIC 1000 based SX module t support Gigabit speeds over 62.5/125 Multi mode Fiber up to a distance of 550 mtrs. |
| **(C) For Multi-mode Fiber (10 / 100 Mbps) for 2 Port** | • Two RJ-45 10 / 100 BASE-TX port ST 100 BASE-FX fiber port<br>• Ethernet Media Converters with no increasing hop count in network<br>• Data Transfer rate - 10/100 Auto Mbps Full Duplex<br>• Fiber Cable : 62.5/125 micron<br>• Cable Length :2 Km or above<br>• UTP Cable Type : Category 5<br>• Indicators<br>Power Indication<br>FX/RX Link Indication<br>UTP/RX Link Indication<br>Full/Half Duplex Indication<br>• Compatibility<br>Standards IEEE 802.3 10Base-T, 802.3u 100Base-TX and 100Base-FX<br>Protocol CSMA / CD<br>• Connection Specification<br>Two RJ-45<br>ST or SC Option, as required |
| **(D) For Single-mode Fiber (10 / 100 Mbps) for 2 Port** | • Two RJ-45 10 / 100 BASE-TX port ST 100 BASE-FX fiber port<br>• Ethernet Media Converters with no increasing hop count in network<br>• Data Transfer rate - 10/100 Auto Mbps Full Duplex<br>• Fiber Cable : 62.5/125 micron<br>• Cable Length :2 Km or above<br>• UTP Cable Type : Category 5 or 6<br>• Indicators<br>Power Indication<br>FX/RX Link Indication<br>UTP/RX Link Indication<br>Full/Half Duplex Indication<br>• Compatibility<br>Standards IEEE 802.3 10Base-T, 802.3u 100Base-TX and 100Base-FX<br>Protocol CSMA/CD<br>• Connection Specification<br>Two RJ-45<br>ST or SC Option, as required |

### 3.2 DSL / ADSL Modems

| DSL / ADSL Modems | |
|---|---|
| **Feature Requirement** | **Product Description** |
| Technology | DSL/ SHDSL/ ADSL/ VDSL etc |
| WAN | Interface - RJ11/RJ45<br>Date Rate - N x 64 Kbps |
| LAN | Interface - RJ 45<br>Ethernet - 1 port 10/100<br>Data Rate - 10/100 Mbps, Full/Half Duplex |
| Console Port | RS-232 or other |
| Memory | Flash RAM & DRAM |
| Transmission Distance | Minimum 2 Km |
| IP Routing Option | Static Routing and RIP v1/RIPv2<br>IP Masquearading (NAT)<br>DHCP Server |
| Bridging | IEEE 802.1d transparent learning Bridge |
| Configuration | Local Console 9RS-232, Telnet, Web (HTTP), Password Control |
| Network Management | SNMP v1/ SNMP v2 agent MIB II |
| PPP | PPP over Ethernet<br>User Authentication with PAP/CHAP/MS-CHAP |
| Firmware Upgrade Option | TFTP or through Remote Facility |
| Trouble Shooting | In Built Diagnostic Facility |
| Other Features Required | One to One DSL Modem Working requirement No separate/Additional Router required Support for DSLAM Integration |

### 3.3 Leased Line Modem

| Leased Line Modem |
|---|
| **G.SHDSL LINE INTERFACE:** |
| Line Code: TCPAM as per ITU-T G.991.2 |
| Line Type: 2-wire (single pair) twisted copper wire. 0.5 mm. Dia.; 2-wire modem should be Upgradeable to 4-wire. |
| Line Impedance: 135 Ohms. |
| Connector: RJ 45 |
| Transmit Signal Power: 13.5 dBm +/- 0.5 dBm |
| Range: Minimum 6 Km on 0.5 mm. Dia. Copper cable @ 2 Mbps in 2-wire; and 7 Kms @ 2 Mbps in 4-wire; 10 Kms at lower speeds. |

| |
|---|
| Line surge protection as per K.20/K.21 |
| **DIGITAL INTERFACE (V.35):** |
| Interface: V.35, 34 pin female connector. |
| Data Rates: 2.304 Mbps (nx64 Kbps, n=1 to 36) |
| Clock: Internal/Recovered from Line. |
| **DIGITAL INTERFACE (G.703/E1):** |
| Line Rate: 2048 Kbps. |
| Line Code: HDB3. |
| Interface: E1 Interface (4-wire) as per CCITT G.703, G.704. |
| Should support Framed and Unframed Channel. |
| Short & Long Haul operation. |
| User selectable CRC4 detection and generation. |
| Programmable Time Slot selection. |
| Impedance: 120 Ohms (Balanced) AND 75 Ohms (Unbalanced). |
| Connector: 1 No. RJ 45 for Balanced OR 2 Nos. BNC for Unbalanced. |
| Clock: Internal/Recovered from G.703. |
| **DIAGNOSTICS:** |
| Local Loop back, Digital Loop back and Remote Digital Loop back. |
| Test Pattern Generator and Checking (BERT). |
| All loop back tests and BERT should be operated through Front Panel switches |
| **CONFIGURATION & MONITORING:** |
| Via DIP Switches, NOT Menu Driven LCD and Keys on Front Panel. |
| Via V.24/RS232 Serial Console Port |
| Via Built-in Ethernet Port with SNMP with Traps and HTTP Agents |
| Monitoring through ICMP Ping. |
| Status monitoring with 15-minute intervals for 30 days. |
| Baud Rate selection from nx64Kbps up to 2048 Kbps. |
| Remote Configuration of slave modem from master modem. |
| **MECHANICAL & ENVIRONMENT** |
| Standalone/ Desktop Unit |
| All Interface cards to be Pluggable & Interchangeable |
| 0 to 50 Deg Celsius, 90% RH Operation |

| **INDICATORS:** |
|---|
| Power, Line Sync, G.703/DTE, BER, Test, TD, RD, Alarm, Low NMR Indication. |
| **POWER:** Dual Mode AC/DC; 230V AC +/- 10%, AND –48 V DC +/- 10%. |

### 3.4 Manageable Switch

| **Manageable Switch (24 Ports/48 Ports)** |
|---|
| **Features:**<br>• **24 Ports/ 48 Ports 10/100/1000 Mbps Switch.**<br>• With Combo mini-GBIC ports (will support 100FX/1000LX /1000SX MiniGBIC transceiver).<br>• Should have VLAN and Trunking support.<br>• Should have SNMPv2 Support.<br>• Should be IPv6 ready with Dual Stacking<br>• Granular Rate Limiting<br>• Min. 14 Link Aggregation Groups with 8 ports on each Group |
| **Specifications:**<br>• IEEE 802.1D Spanning Tree Protocol support for redundant backbone connections and loop-free networks support.<br>• Port Security to secure the access to a port based on the MAC address of a user's device. The aging feature to remove the MAC address from the switch after a specific time to allow another device to connect to the same port.<br>• Multilevel security on console access to prevent unauthorized users from altering the switch configuration.<br>• SNMP and Telnet interface to support comprehensive in-band management, and a CLI management console to provide detailed out-of band management.<br>• Trivial File Transfer Protocol (TFTP) support.<br>• Switch needs to have RS-232 console port for management via a console terminal or PC. |

### 3.5 Manageable POE Switch

| **Manageable POE Switch (24 Ports/48 Ports POE)** |
|---|
| **Features:**<br>• **Should have 24 nos of 10/100/1000 POE ports with additional 2 or more combo ports for 24 Port switch and Should have 48 nos of 10/100/1000 POE ports with additional 2 or more combo ports for 48 Port Switch.**<br>• With Combo mini-GBIC ports (will support 100FX/1000LX /1000SX MiniGBIC transceivers)<br>• Switches should support 802.3af (Should supply 15.4 on all the 24 ports)<br>• Should have SNMPv2 Support.<br>• Should be PoE Class 1 enabled.<br>• Should be IPv6 ready with Dual Stacking<br>• IEEE 802.1Q VLAN encapsulation. Support for 4096 VLAN IDs<br>• Granular Rate Limiting<br>• Support for IEEE 802.3ad Link Aggregation Control Protocol (LACP), Up to 8 groups, Up to 8 ports per group with 16 candidate ports for each (dynamic)<br>• 802.3ad link aggregation<br>• Switching capacity should be min 56 Gbps |

- Forwarding Rate should be more than 38 Millions of Packets per Second (mpps) (64-byte packets)
- 8000 MAC address supported
- IGMP versions 1, 2, and 3 snooping : supports 1K multicast groups
- Packet Buffer should be 4 Mb or more
- Should support Static routing with 512 static routes
- Should Support standard and Extended Access Control List (ACL)

**Specifications:**

- Should Support all the features from Day 1
- Standard 802.1d Spanning Tree support, 802.1w (Rapid Spanning Tree, 802.1s (MSTP).
- Port Security to secure the access to a port based on the MAC address of a user's device. The aging feature to remove the MAC address from the switch after a specific time to allow another device to connect to the same port.
- Multilevel security on console access to prevent unauthorized users from altering the switch configuration.
- IEEE 802.3 10BASE-T/802.3u 100BASE-TX/100FX
- IEEE 802.3ab 1000BASE-T/802.3z 1000BASE-SX/LX
- Port-based and 802.1Q tag-based VLANs, MAC-based VLAN, Guest VLAN, Private VLAN Edge (PVE), also known as protected ports, with multiple uplinks
- Relay of DHCP traffic to DHCP server in different VLAN. Works with DHCP Option 82
- Web/SSL, Telnet server/SSH, ping, traceroute, Simple Network Time Protocol (SNTP), Trivial File Transfer Protocol (TFTP), SNMP, RADIUS, syslog, DNS client, protocol-based VLANs
- IPv6 host mode , IPv6 over Ethernet
- Dual IPv6/IPv4 stack
- IPv6 stateless address auto-configuration
- Duplicate address detection (DAD)
- ICMP version 6
- Switch needs to have RS-232 console port for management via a console terminal or PC.

## 4. LAN/WAN EQUIPMENTS

### 4.1 UPS

1) **600 VA Line Interactive UPS**
2) **1 KVA Online UPS**
3) **2 KVA Online UPS Specification.**

| **600VA Line Interactive UPS (with 15 minutes Battery backup)** | | |
|---|---|---|
| **Sr. No.** | **Parameters** | **Specifications** |
| **1** | General | Single Phase Input & Single Phase Output |
| | | Line Interactive UPS with AVR & PWM Technology for computers suitable for single Phase AC input voltage |
| | | UPS shall be housed in rugged enclosure made of M.S. Sheet 1.2 mm (minimum) thick, aesthetically finished, duly pre-treated and powder coated or ABS body. |

| | | |
|---|---|---|
| | | UPS shall be free from workmanship defects, sharp edges, nicks, scratches, burs etc. All fasteners shall be fixed properly. The equipment shall be complete with all parts and all parts shall be functional |
| | Switching Device | Switching Device shall be MOSFET or IGBT |
| | | Switching frequency shall be above 50 Hz |
| | Transfer time | Switching over time from AC mains to UPS mode on power failure shall be Max. 10 milliseconds |
| | Input | 160 V – 280 V, 50 Hz +/- 3 Hz , single phase AC |
| | Output | |
| | AC Mode | AVR Output voltage in AC mode; 180-255 V ; 50 Hz +/- 3 Hz |
| | Battery Mode | UPS Output voltage in battery mode; 230 V +/- 10%, 50 Hz +/- 3 Hz load power factor of not less than 0.6 lagging |
| | Overload | UPS shall withstand 5% overload |
| | Protections | If input voltage goes outside the range 160V-280V, the system shall switch over to UPS mode |
| | | Over Voltage, short circuit and overload at UPS output terminal, no load shut down. Cold start |
| | | Under voltage at battery terminal, Battery over charge |
| | Indicators and meters | Mains presence, UPS mode, Battery low, overload |
| | Battery details | |
| | Battery Type | Sealed Maintenance Free ( VRLA) Built-in |
| | Battery make | Exide/Quanta/CSB/Panasonic (Battery Sr. No on OEM Letter Head with Warranty Assurance of 1 years) |
| | Minimum Battery AH | 84 VAH – 15 minutes |
| **Online UPS (1 KVA with 30 minutes backup** | | |
| **Sr. No.** | **Parameters** | **Specifications** |
| **2** | | Online UPS with PWM Technology suitable for single Phase AC input voltage |
| | | UPS shall be housed in rugged enclosure made of M.S. Sheet 1.2 mm (minimum) thick, aesthetically finished, duly pre-treated and powder coated. |
| | | UPS shall be free from workmanship defects, sharp edges, nicks, scratches, burs etc. All fasteners shall be fixed properly. The equipment shall be complete with all parts and all parts shall be functional |
| | | Enclosures shall conform to protection requirement of IP2L1 to ISI:3947 (Part 1)/1993 (reaffirmed 1998) |
| | Bypass Switch | Manual and Static by-pass switch shall be provided for maintenance of UPS |
| | | UPS shall supply output power and charging current at the same time |
| | Switching Device | Switching Device shall be IGBT |

| | | |
|---|---|---|
| | | Switching frequency shall be 19 KHz or above |
| | | UPS shall be provided with serial communication port RS 232 for computer interface for data exchange of electrical parameters of UPS like voltage, current, frequency, charging status, mode of operation etc. |
| | **Rating** | The rating specified is a unity power factor |
| | **Input** | |
| | Voltage Range | 160 V – 260 V |
| | Frequency Range | 50 Hz +/- 10% Hz |
| | Phase | Single Phase AC |
| | **Output** | |
| | Voltage Regulation | 230 V +/-2% (with alternative setting for 220V +/- 2%) |
| | Output Frequency | 50 Hz +/- 1 Hz Single Phase (In inverter mode) |
| | Voltage regulation | From on load to full load Should be within +/-1% in both the cases, UPS shall also have facility for operation in synchronous mode in which output frequency shall be same as that of mains frequency |
| | **Harmonic Distortion** | 2% maximum on resistive load for 1 KVA |
| | **Efficiency** | At rated Output voltage and Frequency |
| | Inverter | 90% (min) |
| | Overall | 85% (min) |
| | **Power Factor** | |
| | Load Power Factor | Better than 0.65 lagging |
| | UPS power factor | Better than 0.9 lagging |
| | **Over load** | UPS shall withstand 20% overload for 5 minutes and 50% overload for 1 minute |
| | **Environment** | Noise Level – less than 55 db at a distance of 1 meter |
| | **Protection** | Over voltage, short circuit and overload at UPS output terminal, Under voltage at battery terminal, Overshoot and undershoot shall not be greater than 4% of rated voltage for duration of 60 msec |
| | **Indicators** | Mains Presence, Battery Charging and Discharging, Low battery voltage |
| | **Digital meters** | Input AC Voltage, Output AC Voltage, I/p Current, I/o Frequency, O/p Current & O/p Frequency, Battery Voltage and Current (with LED \ LCD display) |
| | **Battery Detail** | 800 VAH for 1 KVA - 30 min |
| | Battery Type | Sealed Maintenance Free ( VRLA) |
| | Battery Make | Exide/Quanta/CSB/Panasonic (Battery Sr. No on OEM Letter Head with Warranty Assurance of 1 years) |
| | Battery Housing | A suitable battery cabinet matching the UPS enclosures. |

| 2 KVA Online UPS (with 1 hour battery backup) | | |
|---|---|---|
| **Sr. No.** | **Parameters** | **Specifications** |
| **3** | | Online UPS with PWM Technology suitable for single Phase AC input voltage |
| | | UPS shall be housed in rugged enclosure made of M.S. Sheet 1.2 mm (minimum) thick, aesthetically finished, duly pre-treated and powder coated. |
| | | UPS shall be free from workmanship defects, sharp edges, nicks, scratches, burs etc. All fasteners shall be fixed properly. The equipment shall be complete with all parts and all parts shall be functional |
| | | Enclosures shall conform to protection requirement of IP2L1 to ISI:3947 (Part 1)/1993 (reaffirmed 1998) |
| | Bypass Switch | Manual and Static by-pass switch shall be provided for maintenance of UPS |
| | | UPS shall supply output power and charging current at the same time |
| | Switching Device | Switching Device shall be IGBT |
| | | Switching frequency shall be 19 KHz or above |
| | | UPS shall be provided with serial communication port RS 232 for computer interface for data exchange of electrical parameters of UPS like voltage, current, frequency, charging status, mode of operation etc. |
| | **Rating** | The rating specified is a unity power factor |
| | **Input** | |
| | Voltage Range | 160 V – 260 V |
| | Frequency Range | 50 Hz +/- 10% Hz |
| | Phase | Single Phase AC |
| | **Output** | |
| | Voltage Regulation | 230 V +/-2% (with alternative setting for 220V +/- 2%) |
| | Output Frequency | 50 Hz +/- 1 Hz Single Phase (In inverter mode) |
| | Voltage regulation | From on load to full load Should be within +/-1% in both the cases, UPS shall also have facility for operation in synchronous mode in which output frequency shall be same as that of mains frequency |
| | **Harmonic Distortion** | 2% maximum on resistive load for 2 KVA |
| | **Efficiency** | At rated Output voltage and Frequency |
| | Inverter | 90% (min) |
| | Overall | 85% (min) |
| | **Power Factor** | |
| | Load Power Factor | Better than 0.65 lagging |
| | UPS power factor | Better than 0.9 lagging |

| | | |
|---|---|---|
| | **Over load** | UPS shall withstand 20% overload for 5 minutes and 50% overload for 1 minute |
| | **Environment** | Noise Level – less than 55 db at a distance of 1 meter |
| | **Protection** | Over voltage, short circuit and overload at UPS output terminal, Under voltage at battery terminal, Overshoot and undershoot shall not be greater than 4% of rated voltage for duration of 60 msec |
| | **Indicators** | Mains Presence, Battery Charging and Discharging, Low battery voltage |
| | **Digital meters** | Input AC Voltage, Output AC Voltage, I/p Current, I/o Frequency, O/p Current & O/p Frequency, Battery Voltage and Current (with LED \ LCD display) |
| | **Battery Detail** | 3200 VAH for 2 KVA – 60 min |
| | Battery Type | Sealed Maintenance Free ( VRLA) |
| | Battery Make | Exide/Quanta/CSB/Panasonic (Battery Sr. No on OEM Letter Head with Warranty Assurance of 1 years) |
| | Battery Housing | A suitable battery cabinet matching the UPS enclosures. |

**4.2 6U Rack**

1) 6 U wall mounting rack – Rigid frame that can be fixed to the wall,
2) 19'' Adjustable rails in the front and rear,
3) Front section with glass door and lock,
4) Top and bottom cable entry facility,
5) 600mm wide * 500 mm deep, Cable managers, Earth continuity kit, Steel powder coated cabinet (Bidder has to carry out installation/fixing )

**4.3 Power Adaptor**

1) This is a standard Power Adaptor, Input: 230 V AC, Output: 9 V DC, 1A.
2) Output power connector should be compatible to Transreceiver / ADSL modem.

**4.4 Router Specifications:**

| **Router** | |
|---|---|
| **S. No.** | **Requirements** |
| **1** | **General requirements** |
| 1.1 | Router should be modular and should be a single box configuration for ease of management |
| 1.2 | Should have integrated USB port/flash to provide console and storage for configuration/image |
| **2** | **Hardware and interface requirements** |
| 2.1 | Routers should have at least 2 open slots for LAN, WAN modules |
| 2.2 | Routers should support large selective of modular LAN and WAN connectivity options including Gigabit Ethernet and Fast Ethernet, Channelized T1/E1, V.35/G.703 Serial, 3G Wireless(Both HSPA and CDMA) interface modules. |

| | |
|---|---|
| 2.3 | Router should have minimum 4 nos. of 10/100/1000 Gigabit Ethernet ports from day 1 & scalable up to 8 GE Ports for future use |
| **3** | **Performance Requirements** |
| 3.1 | The router should have a minimum performance of 170 Kpps for both IPv4 & IPv6 |
| 3.3 | Should support other IP Services like GRE tunneling, ACLs, IPSEC VPNs, Firewalling, NAT services |
| **4** | **Quality of Service (QoS) requirements** |
| 4.1 | Routers should support Class-based queuing |
| 4.2 | Routers should support marking, policing and shaping |
| **5** | **Routing protocol support** |
| 5.1 | Routers should have IPv4, IPv6, VRRP, Static Routes, RIPv1, RIPv2, OSPFv2, OSPFv3, IS-SI, BGP4, MBGP, BFD, Policy based routing, IPv4 and IPv6 tunnelling enabled from day one |
| **6** | **IPv4 & IPv6 Multicast features** |
| 6.1 | IGMP v1/v2/v3, PIM-DM, PIM-SM, Source Specific Multicast (SSM), MLD V1, V2 |
| **7** | **System Management and Administration** |
| 7.1 | Routers should support Configuration rollback |
| 7.2 | Should support extensive support for SLA monitoring for metrics like delay, latency, jitter, packet loss, RTP-Based VoIP traffic, CRTP |
| **8** | **Security features** |
| 8.1 | Routers should support AAA using RADIUS or TACACS+ |
| 8.2 | Routers should support Packet Filters like: Standard ACL, Extended ACL, ACL that can match arbitrary bits of packet bits of a packet at an arbitrary depth in the packet header and payload |
| 8.3 | Routers should support Network address translation (NAT) |
| 8.4 | Router should be minimum common criteria EAL4 certified |
| **9** | **Built-in troubleshooting** |
| 9.1 | Pre-planned scheduled Reboot Facility |
| 9.2 | Real Time Performance Monitor – service-level agreement verification probes/alerts |

| List of other POPs (45 Nos.) and Addresses | | | | | |
|---|---|---|---|---|---|
| **Sr.N0.** | **Name of District** | **Office Name** | **present mode of connectivity** | **Phone N0.** | **Address** |
| 1 | Ahmedabad | Sarkhej Police Station, Ahmedabad | Wireless | 079-22923559 | Near Sarkhej AMTS Bus Stand, Sarkhej Ahmedabad |
| 2 | Ahmedabad | Shahpur Police Station, Ahmedabad | Wireless | 079-25600545 | Near Shahpur Bahai Centre, Shahpur, Ahmedabad 380 001 |
| 3 | Ahmedabad | Khadia Police Station, Ahmedabad | Wireless | 079-22142828 | Near Raipur Darwaja, Raipur, Ahmedabad 380 022 |
| 4 | Ahmedabad | Office of the State Reserve Police Force, Ahmedabad | Wireless | 079-22823597 | SRPF Group-2 Saijpur Bodha, Ahmedabad |
| 5 | Amreli | Office of the District Superintendent of Police, Amreli | Wireless | 02792-222333 | SP Office Chittal Road , Amreli |
| 6 | Amreli | Agriculture Office. MS Building, Amreli | Wireless | 02792-223345 | Dy. Director, M.S Building,Near Collector Office,Amreli |
| 7 | Anand | Office of the District Superintendent of Police, Anand | Wireless | 02692-260015 | DSP Office, Opp. Jilla Seva Sadan Anand |
| 8 | Anand | Vasad Police Station, Anand | Wireless | 02692-274245 | Near.Railway Station Ta:Anand |
| 9 | Banaskantha | Dist. Mahati Office, Palanpur- Banaskantha | Wireless | 02742-257247 | Dist. Mahati Office,Near Old Gunjbazar,Gathaman gate, Palanpur-Banaskantha |
| 10 | Banaskantha | District Jail Palanpur-Banaskantha | Wireless | 02742-253999 | Dsp Office, Jilaa seva sadan, police Head Courter, District Jail Palanpur- Banaskantha |
| 11 | Bharuch | Sardar Sarovar Narmada Nigam Ltd., Narmada Yogna Vibhag-4 Bharuch | Wireless | 02642-247251 | Executive Engineer Narmada Yogna Vibhag-4 Bharuch |
| 12 | Bharuch | Railway Station, Plat From-1, Bharuch | Wireless | 02642-243766 | Plat From-1 Railway Station, Bharuch |
| 13 | Bhavnagar | Agriculture Office. Navapara Nayab Bagayat ni Kacheri Bhavnagar | Wireless | 0278-2420444 | Technical High School,Navapara Nayab Bagayat ni Kacheri Bhavnagar |
| 14 | Bhavnagar | Office of the District Superintendent of Police, Bhavnagar | Wireless | 0278-2513716 | Dsp Office, Jilaa seva sadan,Joravar palace, Palanpur. Bhavnagar |
| 15 | Dahod | Office of the District Superintendent of Police, Dahod | Wireless | 02643-240944 | DSP Office,Police Headquater Building, Dahod |
| 16 | Dahod | Old Collector office, near Nagar Palika, Dahod | Wireless | 02643-30001 | Gadi Fort near Nagar Palika, Collector Office, Dahod |
| 17 | Gandhinagar | Office of the District Superintendent of Police, sector-27, Gandhinagar | Wireless | 079-23210901 | SP Office, sector-27, Gandhinagar |
| 18 | Gandhinagar | Office of Inspector General, Sector-30 Gandhinagar | Wireless | 079-23260171 | 190/3 JH-Type, Sector-30 Gandhinagar |
| 19 | Jamnagar | Gujarat Maritime Board, Jamnagar | Wireless | 0288-2711803 | Rasool Road ,near Shivam Petroleum Jamnagar |
| 20 | Jamnagar | Civil Hospital, Jamnagar | Wireless | 0288-2554629 | Guru govind sing hospital ,Bedi bandar road, Jamnagar -36008 |
| 21 | Jamnagar | Office of the Anti Corruption Burro, Jamnagar | Wireless | 0288-2551175 | Old Post office Bldg Khambliya naka bahar khoda naka pase Jamnagar |
| 22 | Junagadh | Office of the District Development Officer, Junagadh | Wireless | 0285-2626251 | Jill Panchayat Office , Junagadh |
| 23 | Junagadh | Office of Inspector General, Junagadh | Wireless | 0285-2626550 | Belka road Girivihar SP office Junagadh |
| 24 | Junagadh | District Jail, Junagadh | Wireless | 0285-2620128 | Junagadh Jilla jail sukhnand chokdi-Junagadh |

| Sr.N0. | Name of District | Office Name | present mode of connectivity | Phone N0. | Address |
|---|---|---|---|---|---|
| 25 | Kheda | Railway Police Station, Kheda | Wireless | 0268-2568957 | Railway Police Station, Kheda |
| 26 | Kheda | Office of the District Development Officer, Nadiad-Khead | Wireless | 0268-2557847 | Jilla Panchayat Office,Pavanchakki road,Nadiad-Khead |
| 27 | Kutch | G.K.General Hospital,Bhuj-Kutch | Wireless | 02832-220852 | G.K.General Hospital,Bhuj-Kutch |
| 28 | Kutch | Office of Inspector General, Kutch | Wireless | 02832-232335 | DIG office Mundra Road, Nr.BSNL Office Bhujj , Kutch |
| 29 | Kutch | Collector Campus Bhuj-Kutch | Wireless | 02832-252302 | Collector Campus Bhuj- Kutch |
| 30 | Mehsana | Langanaj Police Station, Mehsana | Wireless | 02762-287337 | Langanaj Police Station, Langanaj Dist Mehsana |
| 31 | Navsari | Agriculture Office, Navsari | Wireless | 02637-282770 | NM Collage Of Agriculture, Aeru char rasta Navsari |
| 32 | Godhra | Civil Hospital, Godhra | Wireless | 02672-243192 | Civil Hospital, Baroda road,Godhra |
| 33 | Patan | Office of the District Superintendent of Police, | Wireless | 02766-231501 | Near Siddhpur circal,on patan-siddhpur road-Patan |
| 34 | Patan | Civil Hospital | Wireless | 02766-233311 | civil Hospital, bhagvada darvaja pase Patan |
| 35 | Rajkot | Office of the Rajkot urban development assotiation, jamnagar road | Wireless | 0281-2476799 | Jamnagar road jam towwer pase chimanbhai patel vikas bhavan prabhat hospital - Rajkot |
| 36 | Rajkot | Office of CP, District Panchayat Chowk, Rajkot | Wireless | 9824518333 | Race Course Ring Road Circle, District Panchayat Chowk, Rajkot |
| 37 | Surat | Office of the District Superintendent of Police, | Wireless | 0261-2479294 | Chokbazar killa,Surat |
| 38 | Surat | Mahidharpura police Station, Surat | Wireless | 0261-2422163 | Mahidharpura Police Station, Station Main Road., Mahidharpura, Surat |
| 39 | Surat | District Jail, Surat | Wireless | 0261-2635404 | Ring Road District Jail Nr.Gujarat Press Surat |
| 40 | Surat | District court | Wireless | 0261-2651802 | District and Sasion, New Court Building, Surat |
| 41 | Surendranagar | Civil Hospital | Wireless | 02752-235106 | Dist. Health Officer, Civil Sergon, Gen. Hospital, Surendranagar |
| 42 | Surendranagar | Joravar Police Station | Wireless | 02752-222052 | Joravarnagar Police Station,Ratanpar Dhal Morbi Bridge Corner, Surendranagar |
| 43 | Vadodara | Railway Station, Plat From-4-5, Vadodara | Wireless | 0265-2344248 | Western Railway Plat Fom No:4-5 Vadodara |
| 44 | Vadodara | Office of the District Development Officer, | Wireless | 0265-2438110 | D.D.O Office. Nr bsnl Office,Vadodara |
| 45 | Valsad | Treasury office, Vapi | Wireless | 0260-2421547 | VIA Char Rasta, GIDC Nr.Bank Of Baroda Silvasa road Vapi, Valsad |

**List of Taluka offices & addresses**

| Sn | District | Taluka | Address |
|---|---|---|---|
| 1 | Ahmedabad | Bavla | Mamlatdar Office, Nr. Rly station, Bavla |
| 2 | Ahmedabad | City | Mamlatdar Office,Ground Floor, Collector Office, Near Subhash Bridge Circle, Ahmedabad. |
| 3 | Ahmedabad | Daskroi | Mamlatdar Office,Ground Floor, Collector Office, Near Subhash Bridge Circle, Ahmedabad. |
| 4 | Ahmedabad | Detroj | Mamlatdar Office, Detroj |
| 5 | Ahmedabad | Dhandhuka | Mamlatdar Office, Opp. Nagarpalika, Dhandhuka |
| 6 | Ahmedabad | Dholera | Mamladar office, Rahtalav Road Dholera |
| 7 | Ahmedabad | Dholka | Mamlatdar Office, Near Railway Station,Dholka |
| 8 | Ahmedabad | Mandal | Mamlatdar Office, Near Bus Stand, Mandal |
| 9 | Ahmedabad | Sanand | Mamlatdar Office, Near Police Station, Sanand |
| 10 | Ahmedabad | Viramgam | Mamlatdar Office,Near Tower, Viramgam |
| 11 | Amreli | Amreli | Mamlatdar Office,Rajmahel Compound, Amreli |
| 12 | Amreli | Babra | Mamlatdar Office, Babra |
| 13 | Amreli | Bagasara | Mamlatdar Office, Gayatrinagar, Bagasra |
| 14 | Amreli | Dhari | Mamlatdar Office, Dhari |
| 15 | Amreli | Jafarabad | Mamlatdar Office, Jafarabad |
| 16 | Amreli | Jesar | Mamladar office, Jesar Seva Sadan Mandali Godown, Opp PGVCL Jesar |
| 17 | Amreli | Khambha | Mamlatdar Office, Khambha |
| 18 | Amreli | Lathi | Mamlatdar Office, Nr.Polce StationLathi |
| 19 | Amreli | Lilia | Mamlatdar Office,Nr.Bus stand Liliya |
| 20 | Amreli | Rajula | Mamlatdar Office, Jawahar Road, Rajula |
| 21 | Amreli | Savarkundla | Mamlatdar Office, Mahuva Road Savarkundla |
| 22 | Amreli | Vadiya | Mamlatdar Office, Vadiya |
| 23 | Anand | Anand (Rural) | Mamlatdar Office, Near Railway Station, Anand |
| 24 | Anand | Anklav | Mamlatdar Office, Kosindra Road, Anklav |

| Sn | District | Taluka | Address |
|---|---|---|---|
| 25 | Anand | Borsad | Mamlatdar Office, Near Nagar-Palika, Borsad |
| 26 | Anand | Khambhat | Mamlatdar Office, Near Tin Darwaja , Khambhat |
| 27 | Anand | Petlad | Mamlatdar Office , Near Sardar chowk, Court Compound, Petlad |
| 28 | Anand | Sojitra | Mamlatdar Office, Near N M high school, Sojitra |
| 29 | Anand | Tarapur | Mamlatdar Office, Near Octroi naka, Tarapur |
| 30 | Anand | Umreth | Mamlatdar Office, Old Chokdi, opp. Santram Mandir , Umreth |
| 31 | Arvalli | Bayad | Mamlatdar office,Nr. Police stationBayad |
| 32 | Arvalli | Bhiloda | Mamlatdar office,Bhiloda |
| 33 | Arvalli | Dhansura | Mamladar office,Dhansura |
| 34 | Arvalli | Malpur | Mamlatdar office,Malpur |
| 35 | Arvalli | Meghraj | Mamlatdar office,Meghraj |
| 36 | Arvalli | Modasa | Mamlatdar office,Modasa |
| 37 | Banaskantha | Amirgadh | Mamlatdar Office, Amirgadh |
| 38 | Banaskantha | Bhanbhar | Mamlatdar Office, Bhabhar-Radhanpur Highway Road, Bhanbhar |
| 39 | Banaskantha | Danta | Mamlatdar Office, Danta |
| 40 | Banaskantha | Dantiwada | Mamlatdar Office, Dantiwada |
| 41 | Banaskantha | Deesa | Mamlatdar Office, Nr.Bagicha, Deesa |
| 42 | Banaskantha | Deodar | Mamlatdar Office, Nr.Dy SP Office, Deodar |
| 43 | Banaskantha | Dhanera | Mamlatdar Office, Opp.GayatriMandir,,Dhanera |
| 44 | Banaskantha | Lakhni | Mamladar office, Gram Panchayat Compound,Lakhni |
| 45 | Banaskantha | Kankrej | Mamlatdar Office, Village Sihori Taluka Kankrej |
| 46 | Banaskantha | Palanpur | Mamlatdar Office, Jilla Sevasadan, Palanpur |
| 47 | Banaskantha | Suigam | Mamladar office, Mahshree Kanad Vidhalya, Bhabhar Road, Suigam |
| 48 | Banaskantha | Tharad | Mamlatdar Office, Bh.Civil Hospital, Tharad |
| 49 | Banaskantha | Vadgam | Mamlatdar Office, Vadgam |
| 50 | Banaskantha | Vav | Mamlatdar Office, Vav |

| Sn | District | Taluka | Address |
|---|---|---|---|
| 51 | Bharuch | Amod | Mamlatdar Office, Jambusar Road, Amod |
| 52 | Bharuch | Ankleshvar | Mamlatdar Office, Near ONGC Circle, Ankleshvar |
| 53 | Bharuch | Bharuch | Mamlatdar Office, Collector Office Campus, Bharuch |
| 54 | Bharuch | Hansot | Mamlatdar Office, Hansot |
| 55 | Bharuch | Jambusar | Mamlatdar Office, Tankari Bhagol, Jambusar |
| 56 | Bharuch | Jhagadiya | Mamlatdar Office, Rajpipla road, Jhagadiya |
| 57 |  | Netrang | Mamlaatdar office  B/H Police Station, Netrang |
| 58 | Bharuch | Vagra | Mamlatdar Office,  Vagara |
| 59 | Bharuch | Valia | Mamlatdar Office, Bus Station road, Valiya |
| 60 | Bhavnagar | Bhavnagar | Mamlatdar Office, Near St. Xevuers High School Jail Road,Bhavanagar |
| 61 | Bhavnagar | Gariyadhar | Mamlatdar Office, Near Polce station,Gariyadhar. |
| 62 | Bhavnagar | Ghogha | Mamlatdar Office, Sahkari madli buldingGhogha. |
| 63 | Bhavnagar | Mahuva | Mamlatdar Office, Court  buliding,Mahuva. |
| 64 | Bhavnagar | Palitana | Mamlatdar office,Hawa Mahel Road Nr. GEB office, Palitana |
| 65 | Bhavnagar | Shihor | Mamlatdar Office, Mainbazar Balmandir, Shihor. |
| 66 | Bhavnagar | Talaja | Mamlatdar office,Talaja. |
| 67 | Bhavnagar | Umrala | Mamlatdar Office, Umarala. |
| 68 | Bhavnagar | Vallbhipur | Mamlatdar Office, Opposite  govt. high school, Vallabhipur. |
| 69 | Botad | Barwala | Mamlatadar Office,Barwala |
| 70 | Botad | Botad | Mamlatadar Office,Botad |
| 71 | Botad | Gadhada | Mamlatadar Office,Gadhada |
| 72 | Botad | Ranpur | Mamlatadr Office,Ranpur |
| 73 | Chota Udaipur | Bodeli | Mamlatadr Office,Bodeli |
| 74 | Chota Udaipur | Chhotaudepur | Mamlatdar Office,Chota-Udepur |
| 75 | Chota Udaipur | Jetpur Pavi | Mamlatdar Office, Nr.Rest House, Jetpur-pavi |
| 76 | Chota Udaipur | Kawant | Mamlatdar Office, Kadipani Road, Kwant |
| 77 | Chota Udaipur | Naswadi | Mamlatdar Office Nasvadi |

| Sn | District | Taluka | Address |
|---|---|---|---|
| 78 | Chota Udaipur | Sankheda | Mamlatdar Office, Sankheda |
| 79 | Dahod | Dahod | Mamlatdar Office, Gadi fort, Nr. Nagar Palika, Dahod |
| 80 | Dahod | Devgadh-Baria | Mamlatdar Office, DevgadhBaria |
| 81 | Dahod | Dhanpur | Mamlatdar Office, Dhanpur |
| 82 | Dahod | Fatepura | Mamlatdar Office,Nr. Pargi Petrol Pump, Fatepura |
| 83 | Dahod | Garbada | Mamlatdar Office,Garbada |
| 84 | Dahod | Limkheda | Mamlatdar Office, Limkheda |
| 85 | Dahod | Jhalod | Mamlatdar Office, Jhalod |
| 86 | Dahod | Sanjeli | Mamlatadr Office,Sanjeli |
| 87 | Dangs | Ahwa | Mamlatdar Office,Collector Office Dangs |
| 88 | Dangs | Subir | Mamlatadr Office,Subir |
| 89 | Dangs | Vaghai | Mamlatadr Office,Vaghai |
| 90 | Devbhumi Dwarka | Bhanvad | Mamlatdar Office,Near police station,Darbarghad, bhanvad |
| 91 | Devbhumi Dwarka | Dwarka (Okha-Mandal) | Mamlatdar Office,Near turiesst banglow, diva dandi, Dwarka |
| 92 | Devbhumi Dwarka | Jam Kalyanpur | Mamlatdar Office,,Jam kalyanpur. |
| 93 | Devbhumi Dwarka | Khambhaliya | Mamlatdar Office,main bazar, khambhaliya |
| 94 | Gandhinagar | Dehgam | Mamlatdar Office, Dehgam |
| 95 | Gandhinagar | Gandhinagar | Mamlatdar Office, Collector Office, 1st floor D Block,Gandhinagar |
| 96 | Gandhinagar | Gozaria | Mamlatadr Office,Gozaria |
| 97 | Gandhinagar | Jotana | Mamlatadr Office,Jotana |
| 98 | Gandhinagar | Mansa | Mamlatdar Office, Superme Chamber, Mansa-Vijapur road,Mansa |
| 99 | Gandhinagar | kalol | Mamlatdar Office,Shivalay complex, Opp GEB office,Mahendra mill road Kalol |
| 100 | Gir Somnath | Girghadha | Mamlatadr Office,Girgadhadha |
| 101 | Gir Somnath | Kodinar | Mamlatdar Office,Nr. Pani Gate, Singavda Nadi kanthe,Kodinar |
| 102 | Gir Somnath | Sutrapada | Mamlatdar Office, Lodva Road, Sutrapada |

| Sn | District | Taluka | Address |
|---|---|---|---|
| 103 | Gir Somnath | Talala | Mamlatdar Office,Talala Gir Dist Junaghar |
| 104 | Gir Somnath | Una | Mamlatdar Office,Gir Ghadhda road,Una |
| 105 | Gir Somnath | Veraval | Mamlatdar Office,Rajendra bhuvan road,Veraval |
| 106 | Jamnagar | Dhrol | Mamlatdar Office, dhrol |
| 107 | Jamnagar | Jamjodhpur | Mamlatdar Office,Taluka Seva Sadan,SVP Highschool Road, jamjodhpur |
| 108 | Jamnagar | Jamnagar | Mamlatdar Office,Lal Bunglow Jamnagar |
| 109 | Jamnagar | Jodiya | Mamlatdar Office,Opp bsnl office, dhrol high way, Jodiya |
| 110 | Jamnagar | Kalavad | Mamlatdar Office,near ST stand Kalavad. |
| 111 | Jamnagar | Lalpur | Mamlatdar Office,Sahkar park, lalpur |
| 112 | Junagadh | Bhesan | Mamlatdar Office, Nr. Old Bus stand Bhensan |
| 113 | Junagadh | Junagadh | Mamlatdar Office, Limda Chowk,Junagadh |
| 114 | Junagadh | Junagadh City | Mamlatadr Office,Junagadh City |
| 115 | Junagadh | Keshod | Mamlatdar Office, Keshod |
| 116 | Junagadh | Maliya-Hatina | Mamlatdar Office,Maliya- Hatina |
| 117 | Junagadh | Manavadar | Mamlatdar Office,Gandhi Chowk,Manavadar |
| 118 | Junagadh | Mangrol | Mamlatdar Office,Mangrol |
| 119 | Junagadh | Mendarada | Mamlatdar Office,Mendarada |
| 120 | Junagadh | Vanthali | Mamlatdar Office,Vanthali |
| 121 | Junagadh | Visavadar | Mamlatdar Office, Nr. Civil court Visavadar |
| 122 | Kheda | Galteshwar | Mamlatadr Office,Galteshwar |
| 123 | Kheda | Kapadvanj | Mamlatdar Office, Kapadwanj |
| 124 | Kheda | Kathlal | Mamlatdar Office,Kapdwanj Road, Kathlal |
| 125 | Kheda | Kheda | Mamlatdar Office, Kheda |
| 126 | Kheda | Mehmadavad | Mamlatdar Office, Mehmadabad |
| 127 | Kheda | Mahudha | Mamlatdar Office,Musafari bunglow, Mahudha |
| 128 | Kheda | Matar | Mamlatdar Office, Matar |
| 129 | Kheda | Nadiad(Rural) | Mamlatdar Office,Opp.Rly Statation Nadiad |
| 130 | Kheda | Thasra | Mamlatdar Office,Nr. Police Station, Godhra Road, Thasara |

| Sn | District | Taluka | Address |
|---|---|---|---|
| 131 | Kheda | Vaso | Mamlatadr Office,Vaso |
| 132 | Kutch | Abadasa | Mamlatdar Office,Nalia ,Ta Abadasa |
| 133 | Kutch | Anjar | Mamlatdar Office, Opp. Bust stand New Anjar |
| 134 | Kutch | Bhachau | Mamlatdar Office, Custom cross road,Bhachau |
| 135 | Kutch | Bhuj | Mamlatdar Office,Taluka Seva Sadan Mundra road ,Bhuj |
| 136 | Kutch | Gandhidham | Mamlatdar Office, Gandhidham |
| 137 | Kutch | Lakhpat | Mamlatdar Office, Viilage Daypar ( 10 km from mata na madh ) ,Lakhapat |
| 138 | Kutch | Mandavi | Mamlatdar Office,Layja Road, opp. Post office Mandvi |
| 139 | Kutch | Mundra | Mamlatdar Office, Mundra |
| 140 | Kutch | Nakhatrana | Mamlatdar Office, Nakhtrana |
| 141 | Kutch | Rapar | Mamlatdar Office, Rapar |
| 142 | Mahisagar | Kadana | Mamlatdar officeNr. Divda colony, Kadana |
| 143 | Mahisagar | Khanpur | Mamlatdar office Village Bakor ta Khanpur |
| 144 | Mahisagar | Lunawala | Mamlatdar office Lunawada |
| 145 | Mahisagar | Santrampur | Mamlatdar office Santrampur |
| 146 | Mahisagar | Virpur | Mamlatadr Office,Virpur |
| 147 | Mahisagar | Balasinor | Mamlatadr Office,Balasinor |
| 148 | Mahesana | Mahesana | mamlatdar office .near azad chok, Mehsana |
| 149 | Mahesana | Unjha | Mamlatdar Office,B/h Tele Exchange ,Mehsana-Siddhipur High way Unjha |
| 150 | Mehsana | Bechraji | Mamlatdar Office,Becharaji |
| 151 | Mehsana | Kadi | Mamlatdar office,opp Meladi matanu mandir, kadi |
| 152 | Mehsana | Kheralu | Mam. Off. Main Bazar, Kheralu |
| 153 | Mehsana | Satlasana | Mamlatdar Office,Station road, Satalasana |
| 154 | Mehsana | Vadnagar | Mam. Off. Near Gang Bazar, Vadnagar |
| 155 | Mehsana | Vijapur | Mamlatdar Office,tower road,Juna bazar Vijapur |
| 156 | Mehsana | Visnagar | Mamlatdar Office, Darbar Road, Visnagar |

| Sn | District | Taluka | Address |
|---|---|---|---|
| 157 | Morbi | Wankaner | Mamlatdar Office, vandha limda chowk, Rasala Road,Vankaner |
| 158 | Morbi | Tankara | Mamlatdar Office,Opp police station, Tankara |
| 159 | Morbi | Morbi | Mamlatdar Office,Taluka seva sadan, Lal Baug,Morbi |
| 160 | Morbi | Maliya Miyana | Mamlatdar Office, Maliyamiana |
| 161 | Morbi | Halvad | Mamlatdar Office, Halvad |
| 162 | Narmada | Dediapada | Mamlatdar Office, Dediapada |
| 163 | Narmada | Nandod | Mamlatdar Office,Lal Tower, Rajpipla |
| 164 | Narmada | Sagbara | Mamlatdar Office,Main Road, Sagbara |
| 165 | Narmada | Tilakvada | Mamlatdar Office,Nr Telephone office, Tilakwada |
| 166 | Navsari | Chikhli | mamlatdar office, chikhli |
| 167 | Navsari | Gandevi | mamlatdar office,Nr. ST Bus deopt,gandevi |
| 168 | Navsari | Jalalpore | Mamlatdar Office,Ground floor collector office, navsari |
| 169 | Navsari | Khergam | Mamlatadr Office,Khergam |
| 170 | Navsari | Navsari (Rural) | Mamlatdar Office,Ground floor collector office, navsari |
| 171 | Navsari | Vansda | mamlatdar office,vasnda |
| 172 | Panchmahal | Ghoghamba | Mamlatdar office ghoghamba |
| 173 | Panchmahal | Halol | Mamlatdar office Halol |
| 174 | Panchmahal | Jambughoda | Mamlatdar office Jambughoda |
| 175 | Panchmahal | Kalol | Mamlatdar office Kalol |
| 176 | Panchmahal | Morva(Hadaf) | Mamlatdar office Morva-hadaf |
| 177 | Panchmahal | Shehara | Mamlatdar office Shahera |
| 178 | Panchmahals | Godhra | Mamlatdar Office,Nr. Mahakali Temple, |
| 179 | Patan | Chanasma | Mamlatdar Office,,Chanasma |
| 180 | Patan | Harij | Mamlatdar Office,Main Bazar,Near Police Station,Harij |
| 181 | Patan | Patan | Mamlatdar Office,Near Kanasada Gate, Bhadra,Patan |

| Sn | District | Taluka | Address |
|---|---|---|---|
| 182 | Patan | Saraswati | Mamlatadr Office,Sarswati |
| 183 | Patan | Radhanpur | Mamlatdar Office,Near Civil Hospital,Radhanpur |
| 184 | Patan | Sami | Mamlatdar Office,Near  vata vas bazar ma,Sami |
| 185 | Patan | Santalpur | Mamlatdar Office,Village Varahi Tal Santalpur |
| 186 | Patan | Sankheshwar | Mamlatadr Office,Sankheshwar |
| 187 | Patan | Sidhpur | Mamlatdar Office, Court compound,Siddhpur |
| 188 | Porbandar | Kutiyana | Mamlatdar Office,Kutiyana |
| 189 | Porbander | Ranavav | Mamlatdar Office Ranavav |
| 190 | Porbundar | Porbundar | Mamlatdar Office,Block No.1, Sandipani Road Opp. Court, Chhaya, Porbandar |
| 191 | Rajkot | Dhoraji | Mamlatdar Office, Darbar Gadh,Dhoraji |
| 192 | Rajkot | Gondal | Mamlatdar Office, Deri Building, Gondal |
| 193 | Rajkot | Jamkandorana | Mamlatdar Office, Nr. Bus stop,Jamkandorana |
| 194 | Rajkot | Jasdan | Mamlatdar Office, Jasdan |
| 195 | Rajkot | Jetpur | Mamlatdar Office, Tin Batti chowk Jetpur |
| 196 | Rajkot | Kotdasangani | Mamlatdar Office, Kotdasangani |
| 197 | Rajkot | Lodhika | Mamlatdar Office, Lodhika |
| 198 | Rajkot | Paddhari | Mamlatdar Office, Nr. Polce Station,Paddhari |
| 199 | Rajkot | Rajkot | Mamlatdar Office, Old Collector Office Compound,Opp. IPMission School, Rajkot |
| 200 | Rajkot | Upleta | Mamlatdar Office, Opp taluka school,Upleta |
| 201 | Sabarkantha | Idar | Mamlatdar office,Idar |
| 202 | Sabarkantha | Khedbrahma | Mamlatdar office,Nr. Old police station opp municiple baro,Khedbrama |
| 203 | Sabarkantha | Posina | Mamlatadr Office,Poshina |
| 204 | Sabarkantha | Prantij | Mamlatdar office,opp. Police station nani bhagodPrantij |
| 205 | Sabarkantha | Talod | Mamlatdar office,Talod |
| 206 | Sabarkantha | Vadali | Mamlatdar office,Vadali |
| 207 | Sabarkantha | Vijaynagar | Mamlatdar office,Vijaynagar |

| Sn | District | Taluka | Address |
|---|---|---|---|
| 208 | Sabarkantha | Himatnagar | Mamlatadar Office,Bahumadi Bhavan, nyay mandir pase,Himmatnagar |
| 209 | Surat | Bardoli | Mamlatdar Office, Nr.Polce station, Sardar ChowkBardoli |
| 210 | Surat | Choryasi | Choryasi Mamlatdar Office, Chok bazar Killa ma , Suratcity |
| 211 | Surat | kamrej | Mamlatdar Office, Kamrej |
| 212 | Surat | Mahuva | Mamlatdar Office, Mahuva |
| 213 | Surat | Mandvi | Mamlatdar Office, Mandvi |
| 214 | Surat | Mangrol | Mamlatdar Office, Mangrol |
| 215 | Surat | Olpad | Mamlatdar Office, Olpad |
| 216 | Surat | Palsana | Mamlatdar Office, Palsana |
| 217 | Surat | Surat City | Mamlatdar Office City Surat, Ghod daud road, valmi campus Nr. Cenal Surat |
| 218 | Surat | Umarpada | Mamlatdar Office, Umarpada |
| 219 | Surendranagar | Chotila | Mamlatdar Office,Opp.Cour  Chotila |
| 220 | Surendranagar | Dasada | Mamlatdar Office, Patdi, Ta Dasada ( Del at Patdi ) |
| 221 | Surendranagar | Dhrangadhara | Mamlatdar Office, Man Mahelat,Dhangadhra |
| 222 | Surendrangar | Chuda | Mamlatdar Office, Chuda |
| 223 | Surendrangar | Lakhtar | Mamlatdar Office, B/h Bus stand,Lakhatar |
| 224 | Surendrangar | Limbdi | Mamlatdar Office,Old jin mill compound, Limbadi |
| 225 | Surendrangar | Sayla | Mamlatdar Office, Sayala |
| 226 | Surendrnagar | Wadhavan | Mamlatdar Office, Wadhavan |
| 227 | Surndranagar | Muli | Mamlatdar Office, Muli |
| 228 | Surndranagar | Thangadh | Mamlatadr Office, Thangadh |
| 229 | Surndranagar | Vichiya | Mamlatadr Office, Vichiya |
| 230 | Tapi | Nizar | Mamlatdar Office , Nizar |
| 231 | Tapi | Songadh | Mamlatdar Office, Police Station Compound, Songadh |
| 232 | Tapi | Uchchhal | Mamlatdar Office, Uchchhal |
| 233 | Tapi | Valod | Mamlatdar Office, Valod |

| Sn | District | Taluka | Address |
|---|---|---|---|
| 234 | Tapi | Vyara | Mamlatdar Office, Vyara |
| 235 | Vadodara | Dabhoi | Mamlatdar Office, Nr.Police Station, Dabhoi |
| 236 | Vadodara | karjan | Mamlatdar Office, Karjan |
| 237 | Vadodara | Padra | Mamlatdar Office, Padara |
| 238 | Vadodara | Sankheda | Mamlatdar Office, Sankheda |
| 239 | Vadodara | Savli | Mamlatdar Office, Savli |
| 240 | Vadodara | Sinor | Mamlatdar Office, Sinor |
| 241 | Vadodara | Vadodara (Rural) | Mamlatdar Office, C Block, 6th Floor, Narmada Bhavan, Jail Road, Vadodara. |
| 242 | Vadodara | Waghodiya | Mamlatdar Office, Vaghodiya |
| 243 | Valsad | Dharampur | Mamlatdar Office,Opp. Old ST Stand,Dharampur. |
| 244 | Valsad | Kaprada | Mamlatdar office, Kaprada |
| 245 | Valsad | Pardi | Mamlatdar office, N.H.8 Pardi |
| 246 | Valsad | Umergaov | Mamlatdar office, Umergaov |
| 247 | Valsad | Valsad | Mamlatdar office, Dharampur Road, Valsad |
| 248 | Valsad | Vapi | Mamlatdar office, Vapi |