No. IV-17017/13/06-Prov.I
Government of India
Ministry of Home Affairs

Jaisalmer House, Man Singh Road,
New Delhi, 15.11.2006

To
The DGs:Assam Rifles/BSF/CISF/CRPF/ITBP/NSG/SSB/BPR&D

Subject:- Finalization of QRs/specifications for Communication Equipments.

The QRs of the following Communication Equipments have been finalized and accepted by the MHA:-

(i) Integration of Voice and Data Communication over Wide Area Network
(ii) Direction Finder

2. Henceforth, all the CPMFs should procure the above items required by them strictly as per the laid down QRs/Specifications.

Alok 16/11/06.
(Alok Mukhopadhyay)
Under Secretary(Prov-I)

Copy to:-

DD(Procurement),MHA

Copy for information to:-

1.PS to JS(PM),MHA
2. Dir(Prov), MHA

PROOPOSAL FOR INTEGRATION OF VOICE / DATA COMMUNICATION OVER WIDE AREA NETWORK FOR BSF

1. INTRODUCTION

The Border Security Force intends to upgrade its existing Voice/data network which caters to messaging and collaboration environment and will address its various requirements mentioned in the subsequent sections. BSF proposes to expand the existing voice/data network to cover approximately 100 additional BSF establishments across the country down to the battalion level. The WAN Infrastructure should support applications including **"INTRANET PRAHARI"**, GIS applications and integration with existing radio NWs.

2. CURRENT INFRASTRUCTURE

Current Network setup is based on 64 Kbps leased line.

The hierarchy of connected establishments is as follows:

a) Center site-Delhi Headquarter
b) Remote site - Frontier Headquarter locations

The current Advance Messaging System is based on Microsoft Windows 2003 & Microsoft Live Communication Server 2005 which takes care of data as well as voice. The routers at 10 Locations are provided with FXO cards which integrate to the EPABX so that existing hardware can be utilized.

Microsoft operations management 2005 is provided so that the server at each location can be monitored for performance and operations. The proposed system should be based on windows and should use the present infrastructure which is MS Exchange, MOM, SMS and LCS. Active directory is being used for centralized authentication and authorization.

3. CURRENT ISSUES

BSF desires to extend the current infrastructure (Phase I) to other locations in Phase II.

Each Frontier location connecting to at least 4-5 sectors.
Each Sector connecting to the at least 4-5 Battalions
Some of the establishment (Frontier/ Sector/Battalions) are
Co-located.
Major Training Institutions will also be connected to Central Site of the Force.

4. BROAD REQUIRMENTS

I. End to end connectivity for Voice, data and video (video up-to Frontiers/Major Training Institutions only.)
II. End to end security on the service provider media.
III. Converged solution for Voice, Data and Video (wherever bandwidth permits).

5. REQUIRED NETWORK INFRASTRUCTURE

Latest hardware/software fully capable to integrate with the existing setup is desirable. Lease line media/ MPLS back bone if feasible, be planned to configure the NW. Competent Govt body approved secrecy is desired to ensure security of information through service provider media.

(a) HQrs to Frontier/ Training Institutions connectivity is required to be upgraded to 2 Mbps leased line/ MPLS from the existing 64 Kbps leased line.

(b) HQrs to Major Training Institutions connectivity is required to 2 MBPS leased line/ MPLS.

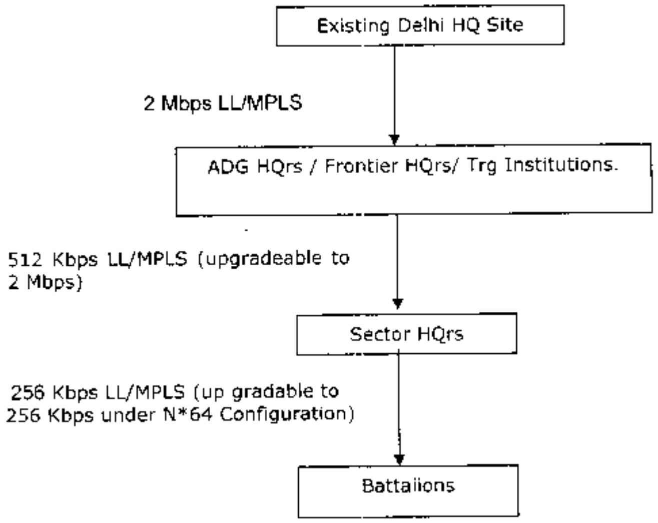
(C) The connectivity between Frontier, Sectors and the battalion will be 128 and 64 Kbps leased line / MPLS respectively.

NOTE: The Routers, Switches and other hard ware component / structure available under the Phase-I be properly utilized during up gradation.

6. LAYOUT FOR UP GRADATION

Hierarchical structure of the organization is as under:

4 - TIER HIERARCHY OF BSF PROPOSED NETWORK


Existing Delhi HQ Site
2 Mbps LL/MPLS
ADG HQrs / Frontier HQrs/ Trg Institutions.
512 Kbps LL/MPLS (upgradeable to 2 Mbps)
Sector HQrs
256 Kbps LL/MPLS (up gradable to 256 Kbps under N*64 Configuration)
Battalions

POINT TO POINT LEASE LINE /MPLS CONNECTIVITY

COMPONENTS OF THE SOLUTION

7. NETWORK TOPOLOGY

NW diagram is enclosed at Fig 1.0. As indicated, Wide Area NW has four hierarchical levels HQ BSF at Delhi, ADG HQrs/ Frontier HQrs/ Trg Insts, Sector HQrs and Battalion HQrs. Since, a number of locations have more than one collocated HQ/Battalion, one media connectivity be planned to support such collocated HQrs/Battalions.

8. MEDIA

Lease Line/ MPLS media is proposed to be used for extension of WAN down to Battalion. Link encryptors at both ends of the service provider media would ensure end to end secrecy on the Wide Area Network for voice, data and video.

9. DATA COMMUNICATION

a) MESSAGING AND COLLABORATION

The main aim of setting up of the advanced messaging solution is to extend high speed data circuit connecting down to Sector HQrs and Battalions so as to integrate all the static location into one network. The planned system should be robust, scalable, reliable, open standard. Secure and allow for on line monitoring.

b) CERTIFICATION

Digital certification server will be incorporated at HQrs New Delhi which will issue private and public key for all the messaging node / user across the country and manage authentication / secrecy of service messages. The certificate authority should be based on windows server2003 R2 and should seamlessly integrate with active directory.

c) CENTRALIZED DIRECTORY SERVICES

AD/LDAP complaint centralized directory services be incorporated.

d) INSTANT MESSAGING

Instant Messaging capability be made available to facilitate chat for online users by using windows live communication server (already existing).

e) FTP (File Transfer Protocol)

The system must be capable to provide a direct mechanism of doing file transfer using the industry standard file transfer protocol.

9. SECURITY

Following be provided to ensure security

- Intrusion detection
- Fire wall transparency
- Strong user authentication
- End to end secrecy on service provider media

10. HARDWARE REQUIREMENT

PROPOSED HARDWARE/ SOFTWARE UP GRADATION IS AS UNDER

(Vender however is at liberty to suggest advance solution if any, without compromising the basic network deliverables)

I) FOR HEADQUARTER LOCATION NEW DELHI

Srl. No.	Product Name	Specification
1.	Router	As attached in Annexure "A"
2.	L3 Switch	As attached in Annexure "D"
3.	Firewall Appliances	As attached in Annexure "E"
4.	Call Manager	As attached in Annexure "F"
5.	Modem	Attached in Annexure "G"
6.	Exchange server with OS /Domain control server with OS/Certification Server with OS/MOM Server with OS/ LCS Server	As attached in Annexure. "H"
7.	Network Management System	As attached in Annexure "K" & "H"
8.	2 KVA UPS	As attached in Annexure "L"
9.	Printer	As attached in Annexure "M"
10.	VC End Point	As attached in Annexure "N"
11.	MCU	As attached in Annexure "O"
12.	Link Encryptor	As attached in Annexure "P

Note: BSF would provide E1 interface on EPABX at Delhi.

II) FOR OTHER LOCATIONS (FRONTIER / SECTOR / BATALLION)

Sl. No.	Product Name	Hardware Specification
1.	Router with Voice Gateway	As attached in Annexure "A & "B".
2.	Layer 2 switch	As attached in Annexure "C
3.	Leased Line Modems 256/512 and 2 Mbps (as required)	Specification attached in Annexure "G".
4.	Additional domain control +Exchange Server.	As attached in Annexure "H
5.	PC	Specification attached in Annexure "J".
6.	2 KVA UPS For Servers, Router, Switch, Modems.	As attached in annexure "L"
7.	600 VA UPS For PC	As attached in annexure "L"
8.	Printer	As attached in annexure "M"
9.	VC End Point	Appendix 'N' (For Frontiers only)
10.	Link Encryptor	As attached in Annexure "P
11.	Cat 5 cable box (of 305 m)/ Cat 5 data i/o with surface mount box/ 24 port jack panel/19" Rack.	As per requirement

Note: BSF would provide E1 interface on EPABX.

ANNEXURE 'A

GENERAL SPECIFICATIONS FOR ROUTERS

It supports minimum of following configuration

1.) Router supports management protocol: SNMP v1/v2/v3, CLI (Telnet/console), TFTP update and configured file management.

2.) All necessary cable (WAN/LAN) to be supplied along with the router.

3.) Router has statefull firewall and 3 DES capability technologies to support the access control strategy based on source & destination IP protocol port & time parameters.

Technical specifications:

One console port

- The router should support USB
- Wire-speed performance for concurrent services such as security and voice , and advanced services to multiple T1/E1/xDSL WAN rates

Shall Support tunneling protocols like IPsec and encryption mechanisms like DES, 3DES, AES (128 and 256 Bit).

- The router should have hardware based encryption to support 3DES/AES and also the routing, Firewall, NAT, QOS, ACL's services together.

- Router has support for the following routing/WAN protocols:
  - PPP /MLPPP
  - HDLC

- Routing protocols support like RIP,OSPF, BGP, VRRP/HSRP, 802.1q , GRE, ACL's and NAT

Shall support the followings

- The router supports statefull packet inspection supporting H.323, SIP and other application level gateway support
- Defense against major "DDOS attacks with policy based NAT/PAT
- Extensive and customizable logging options
- The Statefull firewall supports IPSEC pass through
  Voice traffic optimization with features like LFI, cRTP
- Non-Stop forwarding for fast re-convergence of routing protocols
- boot options like booting from TFTP server, Network node
- multiple storage of multiple images and configurations
- link aggregation using LACP as per IEEE 802.3ad
- VRRP or equivalent
- IPv6 features
- RIPng and OSPFv3 for IPv6
- QoS- Classification and Marking: Policy based routing, IP Precedence, DSCP,
- QoS-Congestion Management: WRED, Priority queuing, Class based weighted fair queuing
- QoS-Traffic Conditioning: Committed Access Rate/Rate limiting
- Link efficiency mechanisms: cRTP, LFI, MLPPP
- multi-level of access
- SNMPv3 authentication

23/9/

• SSHv2 • AAA support using Radius and/or TACACS • PAP and CHAP authentication for P-to-P links • DoS prevention through TCP Intercept • DDoS protection • IP Access list to limit Telnet and SNMP access to router • Multiple privilege level authentication for console and telnet access • Time based ACLs for controlled forwarding based on time of day for offices • IEEE 802.1x support for MAC address authentication • Should have extensive support for SLA monitoring for metrics like delay, latency, jitter, packet loss, and MOS
• Provides QoS features like traffic prioritization, differentiated services, and committed access rate. QoS Support. RSVP/ WFQ/MRED (Multi-level Random early detection). • Router supports for QoS features for defining the QoS policies. Support for Low Latency Queuing. Layer 2 and Layer 3 CoS/DSCP.
• Authentication, Accounting and Authorization services with RADIUS/LDAP/X.509
• Has SNMP monitoring and alerts, Telnet for management and remote management capabilities with encryption. • Shall support Secure Shell • Shall support Out of band management through Console and external modem for remote management
IP Multicast Traffic forwarding Multicast routing protocols support : IGMPv1.v2 (RFC 2236). PIM-SM (RFC2362) and PIM-DM, Multicast VLAN Registration, DVMRP,
The router supports simplified setup with GUI based management
Electrical Power: 200-240 VAC, 50 Hz
Maintenance and Serviceability: Main components of router like motherboard, IO board, power supplies and fan tray should be field replaceable
Cables and accessories: All accessories including data cables, connectors, etc to be provided
Shall be 19" Rack Mountable
Support for HF/VHF /UHF Radio interoperability and integration with VSAT connectivity is required. Future integration will be the responsibility of vender / integrator. For which he has to quote the required hardware/ module including appropriate server as optional.

ADDITIONAL ROUTER CONFIGURATION FOR CENTER SITE

1) Router supports at least minimum sixteen speed synchronous ports (supporting the data rate up to 2 Mbps), 2 ports E1 voice and two 10/100/1000 Mbps high speed Ethernet ports.

2) Should have power supply redundancy. A single power supply should be able to support a fully loaded chassis.

3) Two similar capacity Routers are to be provided at HQ, one for connecting all Frontiers Routers in east and other for connecting all Frontiers Routers in west.

4) The Router should have at least 2 free slots for future expansion.

Technical Parameters:

Router for HQrs
Redundant Power Supply (RPS)
• Shall support at least 400,000pps forwarding performance • Shall support minimum of 64MB flash and 256MB RAM
• The router supports min of 2000 IPSEC tunnels
• Routing protocols like RIP ver1 (RFC1058)&2 (RFC 1722 and 1723), OSPF ver2 (RFC2328), OSPF on demand (RFC1793), BGP4 (RFC1771), IS-IS (RFC1195) • MD-5 route authentication for RIP, OSPF, IS-IS and BGP • Shall support voice call processing locally in the event of the WAN link failure or IP Telephony communication system failure.
Shall support for V.35, E1, E3, G.703, RS232 WAN interfaces, GE as per IEEE 802.3z and 802.3ab,VSAT,FXO,FXS,E1 Voice, E&M
Port requirements : V.35 ports- 16 Nos. 2 Nos- 10/100/1000 Mbps Ethernet ports- One Console Port and 2Xe1 voice

Note: - Synchronous port will be reduced to the actual need for MPLS backbone

26|9|2006

ADDL ROUTER CONFIGURATION FOR FRONTIERS/TRG INSTITUTIONS

It supports minimum of following configuration:

1.) Router has at least eight high speed synchronous ports (supporting the data rate up to 2 Mbps) scalable to twelve. E1 Voice and two 10/100/1000 Mbps high speed Ethernet ports.

The Router should have at least 2 free slots for future expansion

Technical Parameters

Router for Frontier
Redundant Power Supply (RPS)
• Shall support at least 200,000pps forwarding performance • Shall support minimum of 64MB flash and 256MB RAM
• The router supports min of 1000 IPSEC tunnels
• Routing protocols like RIP ver1 (RFC1058)&2 (RFC 1722 and 1723), OSPF ver2 (RFC2328), OSPF on demand (RFC1793), BGP4 (RFC1771), IS-IS (RFC1195) • MD-5 route authentication for RIP. OSPF. IS-IS and BGP • Shall support Voice call processing locally in the event of WAN link / IP Telephony communication system failure.
Supports for ISDN, V.35, E1 WAN interfaces. IEEE 802.3ab, VSAT,FXO,FXS,E&M, E1 Voice
Port requirements : V.35 ports- 8 Nos. 2 Nos- 10/100/1000 Mbps Ethernet ports- One Console Port, E1 voice and redundant power supply

Note: - Synchronous port will be reduced to the actual need for MPLS backbone

ADDITIONAL ROUTER CONFIGURATION FOR SECTORS

it supports minimum of following configuration:

1.) Router has at least six high speed synchronous ports (supporting the data rate up to 2 Mbps). E1 voice and two 10/100/1000 Mbps high speed Ethernet ports.

2.) The Router should have at least 2 free slots for future expansion.

Technical Parameters

Router for Sectors
E1 voice
• Shall support at least 150,000pps forwarding performance
• Shall support minimum of 64MB flash and 256MB RAM
• The router supports min of 1000 IPSEC tunnels
• Routing protocols like RIP ver1 (RFC1058)&2 (RFC 1722 and 1723), OSPF ver2 (RFC2328). OSPF on demand (RFC1793) • MD-5 route authentication for RIP, OSPF • Shall support Voice call processing locally in the event of WAN link / IP Telephony communication system failure.
Support for ISDN, V.35, E1 WAN interfaces. IEEE 802.3ab, VSAT,FXO,FXS,E&M, E1 Voice
Port requirements: V.35 ports- 6 Nos. 2 Nos- 10/100/1000 Mbps Ethernet ports- One Console Port. E1 Voice and redundant power supply

Note: - Synchronous port will be reduced to the actual need for MPLS backbone

26/9/06

ADDL ROUTER CONFIGURATION FOR BATTALIONS

It supports minimum of following configuration:

1.) Router has at least two high speed synchronous ports (supporting the data rate up to 2 Mbps). 2 ports FXO and two 10/100 Mbps high speed Ethernet ports.

2.) The Router should have at least 2 free slots for future expansion.

Technical Parameter:-

Router for Battalions
One high-speed synchronous ports Two ports FXO
• Shall support at least 110,000pps forwarding performance • Shall support minimum of 64MB flash and 128MB RAM. maximum of 128MB flash and 384MB RAM
• The router supports min of 1000 IPSEC tunnels
• Routing protocols like RIP ver1 (RFC1058)&2 (RFC 1722 and 1723), OSPF ver2 (RFC2328), OSPF on demand (RFC1793) • MD-5 route authentication for RIP, OSPF • Shall support Voice call processing locally in the event of WAN link / IP Telephony communication system failure.
Has support for ISDN, V.35, E1 WAN interfaces. IEEE 802.3ab, VSAT, FXO,FXS,E&M, E1 Voice
Port requirements: V.35 ports- 2 Nos., 2 Nos- 10/100 Fast Ethernet ports- One Console Port & 2 ports FXO

Note: - Synchronous port will be reduced to the actual need for MPLS backbone

ANNEXURE 'B'

SPECIFICATIONS FOR VOICE GATEWAY FEATURE AS A PART OF ROUTERS

The voice gateway system at all sites should meet the following specifications

- The voice gateway system should support E1, FXS, FXO and E&M interfaces.
- When a voice gateway router loses contact with the primary IP Telephony System, the gateway should register with the next available IP Telephony System.
- The software on the system must have online software reconfiguration support to ensure that changes made to a gateway configuration take place with immediate effect.
- The system should be capable of booting from a remote node where the image is present.
- The voice gateway should be capable to have removable flash storage for storing software image for high-availability reasons.
- The system should be delivered in such a configuration so that all available channels or timeslots can be used simultaneously for either incoming or outgoing calls using G.711 or G.729a/b CODECs.
- The gateway system should allow the usage of DSP resources by an E1 interface which is not residing on the common interface module.
- Should support H.323 version 4, SIP or MGCP signaling protocols.
- Should support G.711, G.729 and G.729a/b CODECs.
- Should support T.37 Store and Forward Fax and T.38 Fax Relay.
- Should be able to provide call history or records.
- The system should support transcoding functionality between various CODECs (G.711 to G.729) to enable communication between various systems.
- Should support VoIP transport across any layer 1 and layer 2 media.
- Should support following signaling types on the E1 interface – PRI, R2, PRI Q.Sig, CAS for connecting to PSTN/PBX.
- Should support echo cancellation feature as per ITU G.168
- Should provide Silence suppression and voice activity detection service to ensure bandwidth is used only if someone is speaking.
- Should provide comfort noise generation to provide comfort feeling to the phone user that the connection is being maintained, even when no voice packets are being transmitted as VAD is in action.
- Should support hot-line feature so that one pre-defined destination phone should start ringing moment a user picks up an extension configured for hot line.
- Should support automatically busing out a desired voice trunk line PBX when the direct LAN connection to the system is down.
- The gateway should support Direct Inward Dialing (DID) feature
- Should support caller ID and DTMF feature.
- Should support Call Admission Control feature to ensure proper SLA to the user.

- Should support hunt groups across interfaces within the same interface module [illegible] multiple interface modules to ensure calls are forwarded automatically to the first available line.
- Should support CODEC negotiation feature for most efficient usage of bandwidth with desired voice quality.
- Should support VoIP media encryption through Secured RTP (SRTP) as per IETF RFC 3711 for securing VoIP calls.
- Should support H.235 gateway security protocol
- Should support compression of VoIP packet headers using compressed Real Time protocol as per IETF RFC 2508
- Should support IP Precedence and DSCP for VoIP packet classification & marking
- Should have QoS support to offer very low latency and jitter to critical voice traffic
- Should support policing and shaping for delivering the appropriate QoS to applications as well as for securing the voice gateway from threats
- Should support Resource Reservation Protocol (RSVP) as per RFC 2205
- Should support Network Time Protocol (NTP) as per RFC 1305 for time synchronization of the system with the rest of the network.

ANNEXURE 'C'

SPECIFICATION FOR 24 PORT MANAGED LAYER-2 SWITCH

- The switch should have 24 nos of 10/100BaseTX interfaces and 2 nos of uplink consisting of 1000BaseT interfaces.

- All of the above 26 interfaces should be activated simultaneously.

- The switch should have 8Gbps switching and forwarding rate of 6.5Mpps using 64-byte packet size for non blocking performance.

- The switch should support for minimum 8,000 MAC addresses

- Support IEEE 802.1Q VLAN and 802.1d STP; IEEE 802.1s and 802.1w for spanning tree enhancements

- Should link aggregation to increase the performance of the switch.

- It should be possible to have the VLAN configuration done centrally. To achieve it, the switch should have the feature that enables addition, deletion, and modification of VLANs for all switches in the LAN by just configuring this switch only.

- The following standard compliance is required on the switch - 802.1x; 802.1x user authentication with VLAN assignment, port security & guest VLAN; 802.1x accounting.

- Should support local and central management.

- Support for port based security to prevent unauthorized stations from accessing the switch by restricting the number of MAC addresses allowed to access the port as well as by statically configuring the MAC address

- Support for AAA, RADIUS.

- Should Support SNMPv1, SNMPv2c, SNMPv3, Console, RMON, CLI, Remote Monitoring Should support Secured Shell (SSH) for secured access to the switch

- Should support IEEE 802.1p class of service (CoS)

- Should support traffic classification & marking.

- Supports 4 Groups of RMON.

- Should support per-port broadcast, multicast and unicast storm control to prevent faulty and stations sending broadcast/ multicast/unicast, which can degrade overall network performance.

- Should support redundant power supply.

28/9/10

ANNEXURE 'D'

SPECIFICATION FOR 48 PORT MANAGED LAYER-3 SWITCH

- The switch should have 48 nos of 10/100/1000 Base TX interfaces and configurable 4 hot pluggable GBIC/SFP Support for 1000BaseSX, LX & ZX interfaces.

- All of the above 52 interfaces should be activated simultaneously.

- The switch should have 90Gbps switching and forwarding rate of 70Mpps using 64-byte packet size for non blocking performance.

- The switch should support for minimum 32,000 MAC addresses

- Support IEEE 802.1Q VLAN and 802.1d STP: IEEE 802.1s and 802.1w for spanning tree enhancements

- Should link aggregation to increase the performance of the switch.

- The switch should support detection of uni-directional fiber links to avoid network performance disruption.

- Should have redundant power supply.

- It should be possible to have the VLAN configuration done centrally. To achieve it, the switch should have the feature that enables addition, deletion, and modification of VLANs for all switches in the LAN by just configuring this switch only.
- Should ACLs on all ports The ACL parameters may be any combination of source and destination IP or subnet, protocol type (TCP/UDP/IP etc), source and destination port.
- The following standard compliance is required on the switch - 802.1x; 802.1x user authentication with VLAN assignment, port security & guest VLAN: 802.1x accounting.
- Should support DHCP snooping to provide security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding table.
- Should support implementation of control configuration on the switch to ensure SNMP access only to the SNMP manager or the NMS workstation through access lists.
- Should support configuring access lists to restrict telnet or SSH access.
- Should support per port broadcast, multicast and unicast storm control to prevent faulty end stations from degrading overall system performance.
- Support for port based security to prevent unauthorized stations from accessing the switch by restricting the number of MAC addresses allowed to access the port as well as by statically configuring the MAC address
- Support for AAA, RADIUS and TACACS as per RFC 1492.
- Should Support SNMPv1, SNMPv2c, SNMPv3, Console, RMON, CLI, Remote Monitoring Should support Secured Shell (SSH) for secured access to the switch
- Should support IEEE 802.1p class of service (CoS) and Differentiated Services Code Point (DSCP) for QoS policies
- Should support traffic classification & marking.
- supports 4 Groups of RMON

28/5/12

ANNEXURE 'E'

FIREWALL SPECIFICATIONS

Key Specifications

- The appliance based security platform should be simultaneously capable of providing firewall and IPSec & SSL VPN.
- It should be a single chassis solution.
- Should support both AC and DC power supply option.
- The security appliance should have at least 4 nos of 10/100/1000BaseTX interfaces and shall support additional 4 nos of 10/100/1000BaseTX or 1000BaseSX or 1000Base LX interfaces
- Should have a 10/100BaseTx interface for out-of-band management purpose.
- The platform should be based on real time, secure, embedded operating system
- The appliance should have in-built support for IPSec VPNs with DES, 3DES. AES (128 & 256bit) encryption.
- Shall support at least 40 virtual firewall solution, every firewall context should have its own management and syslogging.
- Should have USB ports.

High Availability Requirements

- The solution should have two appliances in failover mode with no single point of failure or session loss in an event of the primary platform failure
- Should provide active-active as well as active-standby configuration for firewall failover.
- Should support LAN based failover option to support geographic separation of the appliance within the campus for higher availability.
- Should support asymmetric routing topologies so that traffic flows can enter through primary appliance and exit through the secondary appliance if need arise.
- On power up the platform should use built-in system monitoring & diagnostics before going online to detect failure of hardware.
- The platform should support stateful failover to prevent session losses for firewall operation.
- IKE keepalive should be supported that allows the devices to detect a dead remote peer for IPSec redundancy.
- The software on the platform should support online software reconfiguration to ensure that changes made to a platform configuration take place with immediate effect.
- It should be possible to upgrade the software of the appliance without disrupting the services.

Performance Requirements

- Should support unlimited users for firewall services.
- The security appliance should support firewall throughput of at least 600Mbps
- Should support a IPSec 3DES and AES throughput of at least 300Mbps
- Should support at least 500 IPSec and SSL VPN peers in the delivered configuration. The number of such VPN peers should be scalable upto at least 2000 for both IPSec and SSL.
- Should support at least 275,000 concurrent sessions. New session creation support should be at least 20,000 sessions per second
- The security appliance should support at least 100 Virtual LANs.
- The security appliance should have at least 1GB of RAM. 64 MB Flash and maximum of 512 MB Compact Flash.

Feature Requirements

- Should support RIP Version 2, and OSPF routing protocols.
- Should support MD5 based authentication for both RIP and OSPF

- Should support DHCP server & DHCP Relay Agent functionality
- The platform should support for Static & Dynamic Network Address Translation and also Port Address Translation
- Should support NAT Transparency
- Should support AES 128, 192 and 256 bit key sizes
- The appliance should support VLAN and 802.1Q Tagging
- Should have IPv6 networking feature. Should support dual stack of IPv4 and IPv6.
- Should support IPv6 ACL to implement security policies for IPv6 traffic.
- Should support layer 2 transparent firewall mode where both side of the firewall should belong to the same IP subnet. While the firewall is working in layer 2 transparent mode, it should still provide layer 2-7 security services and should protect the system from network layer attacks.
- Should support access control based on layer 2 ether type field to enable security implementations at layer 2.
- Should support IP Multicast through IGMP and PIM to support secure real-time multicast application which will have to pass through the firewall.
- The firewall will have to provide QoS service to ensure guaranteed bandwidth, delay and jitter for real-time and mission critical traffic like voice over other non-mission critical traffic.
- Should support dynamic downloading and enforcement of ACLs on a per-user basis once the user is authenticated with the appliance.
- Should provide application inspection services for applications like HTTP, FTP, SNMP, DNS, SMTP, NFS, LDAP etc.
- The security appliance should be able to protect the port-80 misuse to block applications such as Instant Messaging like yahoo messenger, MSN messenger etc.
- Should be able to block popular peer-to-peer applications like Kaaza.
- Should be able to inspect HTTP and FTP traffic when these are deployed using non-standard ports i.e. when HTTP is not using port TCP/80 and FTP is not using port TCP/21.
- Should support the following HTTP security services - RFC compliance, protocol anomaly detection, protocol state tracking, MIME type validation, Uniform Resource Identifier (URI) length enforcement
- Should support the following FTP security services - protocol anomaly detection, protocol state tracking, NAT and PAT support, and dynamic port opening & closing. The appliance should have the capability to enforce what operations users and groups can perform within FTP sessions.
- Should support IPv6 application inspection for HTTP, FTP.
- Should support application inspection of following type of multimedia traffic - H.323 version 3 and 4, SIP, MGCP, RTSP, TAPI and JTAPI.
- Should support the following H.323 security services – H.323 v3 & v4 with Direct Call Signaling and Gatekeeper Router Control Signaling, NAT & PAT support for H.323 services.
- Should support the following SIP security services – ability to secures both UDP and TCP based SIP environments, NAT & PAT based address translation support for SIP phones.
- Should support inspection of H.323 and SIP voice traffic that has been fragmented.
- Should support TCP stream reassembly and analysis, TCP traffic normalization, flag and option checking, TCP packet checksum verification services.
- Should be able to protect "ARP spoofing" attacks at layer 2 by ARP inspection to prevent malicious users from impersonating other hosts.
- Should support HTTP, HTTPS and FTP filtering. Should support Java and Active-x filtering.
- Should support time based access list to control the usage of application and resources based on time parameters.
- Should support site-to-site and remote access IPSec VPN & SSL VPN. The bidder should provide VPN client with unlimited user license along with every security appliance for all sites.
- The firewall should supports SNMP v1, V2c and V3.

26\9\12

- Remote network access to the firewall is only possible through the secure access.
- Firewalls should manageable from a centralized Solaris/Windows administration station
- The firewall administration station is capable of pushing firewall security policies and configurations to individual or multiple firewalls through a secure, encrypted connection to the firewall administration interfaces
- The firewall shall provide a Graphical User Interface (GUI) and a Command Line Interface (CLI) for making changes to the firewall rules set. Access to the firewalls via the GUI or the CLI must be through an encrypted channel

Multimedia support

- Microsoft NetShow, White Pine CU-SeeMe, RealNetworks RealAudio. H.323. SIP, RTSP application inspection support.

26/9/2006

ANNEXURE 'F'

SPECIFICATIONS FOR CALL MANAGER

The IP Telephony communication system should be an integrated telephony solution for Analog & IP Phones, gateways over IP architecture and should be scalable to support upto 1000 users.

- The IP Telephony communication system at the HQ should support redundant solution capable of providing 1:1(server to server) redundancy to all IP phones in the network. This would ensure reduction in downtime for the end devices/phones. The bidder should provide a detailed description of the call flow of their system.
- If the primary appliance(s) of the IP Telephony system fails, all end points (IP and analog phones) should automatically register themselves with the backup appliance(s) of the IP Telephony System without any manual intervention.
- No existing calls should be dropped during the switchover mentioned in the above point if the link is alive between them (2 sites on call).
- The telephony user shall not do anything/any configuration (no manual intervention) to revert to the active server from the failed server.
- Should support for fax communication also across for sending the printed documents. All the offices should have provision for one analog port for Fax machine connectivity.
- The IP Telephony solution must ensure that per call bandwidth consumed over the WAN is not more than 14Kbps on E1 links. The bidder should provide a detailed description of the mechanisms deployed to achieve the desired per call bandwidth.
- Should provide the directory of all users of the region so that the users can search the using their IP Phones on the directory by first name or last name and can make calls to them.
- The users should be able to configure their own settings for their phone like speed dials, call forward settings etc through web interface without the intervention of the administrator.
- Should provide Secure HTTP (HTTPS) support for management interface and user interface through which user changes his own settings.
- Should support configuration of an authorization code that has to be entered by user prior to extending a call to a specific route pattern for enhanced security and to prevent toll frauds. The CDR should capture the details of the authorization code usage.
- Should provide QoS statistics on a per call if needed.
- The IP telephony solution should have CODEC support for G.711 @ 64kbps, G.729A/B @ 8kbps. The compression codecs will be required for efficient utilization of the bandwidth resources.

Administrative Features:

- Call detail records
- CDR Analysis and Reporting Tools
- Centralized, replicated configuration database, distributed Web based management
- Configurable Call Forward Display
- Database automated change notification

- Date and time display
- Lightweight Directory Access Protocol (LDAP) Version 3 directory interface to selected vendor's LDAP directories
  i. Active Directory
  ii. Netscape Directory Server
- Debug information to common syslog file
- Device-downloadable feature upgrades--Phones, hardware transcoder resource, hardware conference bridge resource, VoIP gateway resource
- Dynamic Host Configuration Protocol (DHCP) block IP assignment— Phones and gateways
- Dialed Number Analyzer (DNA)
- Dialed number translation table (inbound and outbound translation)
- Dialed number identification service

User Features

Abbreviated Dial
Answer and answer release
Barge
Callback busy, no reply to station
Call connection
Call coverage
Call forward--all (off net and on net)
Call forward—busy
Call forward—no answer
Call hold and retrieve
Call Join
Call park and pickup
Call pickup group-universal
Call status per line (state, duration, number)
Call waiting and retrieve (with configurable audible alerting)
Calling Line Identification
Calling Line Identification Restriction call by call
Calling party name identification
Conference Barge
Conference List and Drop any party
Direct inward dial (DID)
Direct outward dial (DOD)
Directory dial from phone—corporate, personal
Directories—missed, placed, received calls list stored on selected IP phones
Distinctive rings
Distinctive ring per phone
Drop last conference party (ad-hoc conferences)
Extension mobility support
Hands-free, speakerphone
Immediate Divert to voicemail
Last numbers redial
Malicious Call ID and Trace

IP Phone

- Six interactive/programmable soft keys.
- High-quality duplex speakerphone, handset, and headset.

- The display should provide features such as date and time, calling party name, calling party number. and digits dialed
- Select background images
- Unique ringer sounds
- The corporate directory integration with the Lightweight Directory Access Protocol Version 3 (LDAP3) standard directory.
- Configuration should be done either automatically or manually set up for Dynamic Host Control Protocol (DHCP
- Internal 2-port 10/100BaseT Ethernet switch
- Phone must have a large, high-resolution display with a min size of (320 x 220).
- G.711µ and G.729a audio compression codecs differentiated services code point (DSCP) and 802.1Q/p standards.
- IEEE 803.af PoE, option of locally powering with a power supply
- Support for digital certificates. device authentication, and encryption.
- Comfort-noise generation and voice activity detection (VAD) programming support.
- Should support SIP or SCCP Signaling Protocol.

ANNEXURE 'G'

TECHNICAL SPECIFICATION OF G.SHDSL MODEM

Modem Supports :

- Software Download Firmware
- Remote Download Firmware
- Multi-color LED indicators
- Each unit can be set to be either master or slave

G .SHDSL LINE INTERFACE

- Full duplex with adaptive echo cancellation 16PAM line coding
- Unconditioned 19-26 AWG twisted pair
- supports ITU-T G.991.2
- Line type: 2 wire (single pair), twisted copper wire. 0.5 mm dia; upgradeable to 4-wire
- Connector; RJ 45

Router Interface

- Number of Ports 1
- Physical Interface 10/100 Base-T
- Connector RJ45
- Supported Routing
- Protocol RIP-I, RIP-II
- Data Rate N x 64 Kbps up to E1 capacity, 15,000 frames per second
- Supported Protocols TCP/IP, PPP, HDLC
- PPP

Clock: xDSL looped, Internal,

Console Port

- Connector DB9S at front panel
- Electrical RS232 interface (DCE)
- Protocol Menu driven VT-100 terminal

System Configuration Parameters (All in non-volatile memory)

Active Configuration	Current working configuration
Default Configuration	Manufacture default configuration

Diagnostics Test: Loop back test

Front Panel

- Keypad 4 keys:
- LCD panel
- LED Indicators

Electrical specifications:

230 V AC +/- 10% 50 Hz +/- 5%

TECHNICAL SPECIFICATION OF 2 MBPS MODEM

Modem supports:

- Software Download Firmware
- Remote Download Firmware
- Multi-color LED indicators
- Each unit can be set to be either master or slave

G .SHDSL LINE INTERFACE

- Line Code 16/32-TCPAM, full duplex with adaptive echo cancellation
- Electrical Unconditioned 19-26 AWG twisted pair (MODEM SHOULD SUPPORT 2 WIRE AS WELL 4 WIRE)-
- Connector RJ45 -

E1 Interface

- Line Rate 2.048 Mbps ± 50 PPM Framing ITU G.704
- Line Code HDB3 Connector BNC/RJ48C
- Input Signal ITU G.703 Output Signal ITU G.703

DTE Interface

- Data Port Single DTE
- Data Rate n x 64 Kbps (up to line rate)
- Connector M34 connector for V.35 interface.

Clock: xDSL looped, Internal,

Console Port

- Connector DB9S at front panel -
- Electrical RS232 interface (DCE)
- Protocol Menu driven VT-100 terminal

System Configuration Parameters (All in non-volatile memory)

- Active Configuration Current working configuration
- Default Configuration Manufacture default configuration

Diagnostics Test: Loop back test

Front Panel

- Keypad 4 keys
- LCD panel.
- LED Indicators

Physical/Electrical

- 230V AC+/- 10% and 48 V DC +/-5%

TECHNICAL SPECIFICATION OF 64/128 KBPS MODEM

Features:

- Up to 9.0KM distance over unconditioned 24 AWG wires.
- High Speed DTE interface up to 128 Kbps synchronous.

Line Interface

- Type Full duplex with adaptive echo cancellation
- Line Coding 2B1Q
- Line Type Unconditioned twisted pair 19-26 AWG
- Surge Protection Meets FCC Part 68 Subpart D
- Connector RJ48

DTE Interface (V.35)

- Number of Port 1
- Data Rate 64 and 128 Kbps synchronous
- Connector M34

Co-directional Interface

- Interface ITU G.703 64 Kbps co-directional interface
- Connector 120ohm, RJ48
- Line Distance Up to 500 meters
- 300 Mtr. Standrad
- Loop back DTE Payload Loop back, DTE to Line Loop back
- **Clock source** Internal, Line, or DTE

Diagnostics Test

- Loopbacks Near Payload Loopback and DTE to DTE Loopback

Electrical

- Power 100-240 VAC

24/9/2005

ANNEXURE 'H'

HIGH END SERVER SPECIFICATION
HQ/Frontier

HARDWARE

Processor : One Intel Xeon Processor MP at 3.00 GHz/8MB
Cache Memory : 8-MB Integrated Level 3 cache (per processor)
Upgradability: Upgradable to quad processing
Chipset : Intel® E8500 chipset
Memory Protection: Hot-Plug RAID Memory ,Hot-Plug Mirrored Memory ,Online Spare Memory
Memory: **4 GB PC2-3200R** MHz Registered ECC SDRAM DIMM Memory. Maximum upgradable to 48 GB
15" Col Monitor
Network Controller: Embedded Dual Port PCI-X 10/100/1000T Gigabit network adapter
PCI Expansion Slots: Min 5 nos. of PCI 64 bit 100 Mhz PCI – X slots, Min 4 nos. of PCI express slots.
Storage Controllers: Integrated Dual Channel Wide Ultra3 SCSI Adapter
Storage: Diskette Drives : 1.44 MB Slimline Drive. Optical Drive :DVD-ROM Drive
Hard Drives: **2 nos** of 72GB 15k rpm HDD with the capability of duplexing on a split backplane with DVD R/W drive
Internal Storage Type: Min 8 Nos of Duplexed Hot plug drive bays (4+4)
Interfaces: Parallel-1, Serial-1, Front USB Port-1,Rear USB Ports-2,Network RJ-45-2, External SCSI -1
Graphics: Integrated ATI RAGE XL Video Controller with 8MB Video Memory
Form Factor: Tower or Rack (6U) WITH Rack mounting kit
Industry Standard Compliance: ACPI 2.0 Compliant. PCI 2.2 Compliant, PXE Support
WOL Support, Physical Address Extension (PAE) Support. FCC / UL Standards Compliant.
The server should have been audited / benchmarked by transaction processing council (www.tpc.org) for performance.

Availability features

- Advanced ECC Memory to detect and correct 4bit memory errors that occur within a single DRAM chip on a DIMM in combination with industry standard ECC DIMMS.
- Hot Plug Mirrored Memory
- PCI-X Hot Plug Technology
- Two 600W Hot Plug Power Supply
- Six Hot Plug System Fans

Manageability

Intelligent Manageability
Virtual Text Remote Console
Virtual Power Button Control
Hardware Based Remote Management
Automatic Server Recovery-2
Integrated Management Log (IML)
Off-Line Backup Processor capability
Dynamic sector repairing and drive parameter tracking
Redundant/adaptive load balancing NIC Support

Remote Manageability

Hardware based. Operating System Independent Remote Management controller card, having Integrated Management Log & Support for multiple user accounts with customizable access privileges with SSL level security and provide Virtual graphical Text Remote Console , Virtual Power Button & media Control e.g.Remote Insight Board, Remote supervisory adaptor from IBM etc.

Management Software:

Server OEM Browser based Management Software for Monitoring, Managing and Configuring Servers. The management should support Query based monitoring of the server components. Support for heterogeneous operating environments - Microsoft Windows 2000, Microsoft Windows NT. Queries and tasks enable the creation of customized views of devices and events and self-updating polling, notification, and control tasks. Provides comprehensive fault/performance management and robust system software version control and distribution.

The Management software should also support Integration with Microsoft Systems Management Server. etc.

Performance Analysis Software

The software should be able to analyze and graphically display performances of CPUs & Memory at a given time and over a period of time as well. It should be capable to generate reports of these performances in order to determine performance bottlenecks and trouble shooting.

SOFTWARE

OPERATING SYSTEM	:	WINDOWS 2003 R2 WITH SA
DIRECTORY SERVICES	:	ACTIVE DIRECTORY
MESSAGING SYSTEM	:	EXCHANGE 2003 WITH SA
SYSTEM MANAGEMENT	:	SYSTEM MANAGEMENT SERVER WITH SA
MANAGEMENT	:	MICROSOFT OPERATION MANAGER WITH SA
COMMUNICATION & COLABARATION	:	MS LIVE COMMUNICATION SERVER WITH SA
PKI	:	WIODOWS 2003 R2 BASED
DATA BASE	:	SQL SERVER 2005 WITH SA

NOTE: - Appropriate Software would be provided to engineer / configure the service.

22/3/12

ANNEXURE 'I'

LOW END SERVER SPECIFICATION (Sector/Battalions)

- Intel Xeon processor at 3.4GHz with 2MB cache, 800MHz FSB and server class chipset such as E7520
- 2 GB of 400MHz ECC DDR SDRAM expandable to min 12 GB
- Dual channel Ultra-320 SCSI controller
- At least 4 nos 64-bit PCI-X slots distributed on at least 2 nos PCI-X buses with no embedded devices on these buses for best performance
- At least 2 nos 64-bit PCI-express slots for high performance
- 3 nos of 72GB 15k rpm HDD with the capability of duplexing on a split backplane
- 2 x Gigabit network card
- 15" Col Monitor
- Dual channel RAID controller with 64MB cache for RAID 5
- Redundant power supply of at least 600W each
- Redundant fan sub-systems
- Manageability software
- Management Software should be a Browser based Interface from the OEM vendor itself and should not be a third party management tool.
- Capability of doing Asset Tracking including Serial Numbers of the server and server sub-components is required.
- Should be capable of Change management and version control for System Software including system hardware drivers, ROM updates and patches
- Should be capable of integrating by means of agents into NMS such as HP Openview, CA Unicentre and Tivoli.
- Should be capable of managing all vendor devices including desktops, servers etc and also third party devices from the same interface
- Redundant ROM, ROM based Setup Facility, Remote Flash ROM
- Automatic Server Recovery 2, Advanced Server Management feature
- Pre-failure alert AND Warranty for Processor, Memory and Hard disks.
- Support for PXE boot & WOL.
- Dedicated Ethernet Port for Hardware based, OS Independent SSL encrypted out of band remote management.
- Backup DAT device with capacity of 36/72GB with capacity for booting off the tape device in case of a disaster
- Operating system – Windows 2003 R2 or higher.

Standards

The vendor should produce documentation that the server is listed on the website of the tpmC council..

The server should comply to FCC /UL standards

OS certification

The vendor should produce documentation that the server is listed on the website of the respective OS vendor.

Windows 2000, 2003. Netware, Linux (Red Hat Ent 3.0)

PERSONAL COMPUTER SPECIFICATION

S.No.	Feature	Detailed Specification
1	Processor	Intel Conroe E6300 1.86GHz, 4MB L2 Cache, 1066 MHz FSB or above
2	Chipset	Intel 963 Series Chipset
3	Motherboard	**OEM or Intel mother board**
4	Memory	512 MB **DDR2 SDRAM @ 533 MHz** Expandable to 4 GB
5	Floppy Drive	No Floppy Drive
6	Hard Disk Drive	160 GB SATA-II (3GBps transfer rate) **SMART III** 7200 rpm with pre failure Alert
7	Optical Drive	48X/32X Combo CD-RW/DVD-ROM Drive
8	Graphics	Integrated (on board) Intel GMA 950
9	Audio	Integrated (on board) **High Definition Audio** controller with internal speaker
10	Ethernet	Integrated (on-board) 10/100/1000 controller
11	Bays	3 or more
12	Slots	4 or more
13	Ports	1 Parallel, 1 Serial, 8 USB (Ver 2.0) with at least 2 ports in front, rear ports - VGA, Speaker, Microphone, Headphone. 2 PS/2 ports , one RJ45 network port
14	Form Factor	Small Form Factor / Microtower
15	Power Supply	250 Watts (Surge protected)
16	Monitor	17" Color with minimum 1280 x 1024 @ 60Hz resolution **with FCC, UL, MPR II/TCO and Win XP certification. Energy Star compliance. (Same make as PC)**
17	Keyboard	**PS/2** 104 keys keyboard **(Same make as PC)**
18	Mouse	**PS/2** 2 Button **Optical Scroll** Mouse **(Microsoft or OEM)**
19	Operating System	**Pre installed Microsoft Windows XP Pro SP2 with OS CD, documentation CD with each PC**
20	Drivers for different Operating systems	**Drivers should be freely available on OEM's web site**
21	Security	1. Removable media boot control 2. Serial, Parallel & USB Interface Control 3. Power-On Password 4. Setup Password
22	Compliance And Certification to be submitted	**For OEM : ISO 9001:2000** **For PC : FCC, UL ,Win XP and Linux certification** **For Monitor : Energy Star compliance, UL, FCC MPR II/TCO and Win XP certification**

ANNEXURE 'K'

NETWORK MANAGEMENT SYSTEM (NMS) SPECIFICATION

1. *Network Management*

1.1.1. Network Management Server (One at Central Location), setup as Master station.

1.1.2. Network Management Station (One at each regional center), setup as collection station.

1.1.3. Central Management station should act as backup of the regional management station.

1.1.4. Filtering of events that are passed between collection station and master station should be possible.

1.1.5. Data synchronization between collection station and master station should be based on hours scheduled by administrator

1.1.6. Each regional center shall have full control of the network management station in their location.

1.1.7. NMS shall provide secured windows based consoles as well as secured web-based consoles.

1.1.8. The NMS shall provide tight integration of fault and configuration functions of element managers like Cisco Works 2000, Nortel Optivity, Entrasys manager.

1.1.9. The solution should provide for future scalability of the whole system without major architectural changes. Therefore the system should support distributed hierarchical architecture

1.1.10. Polling intervals should be configurable on a need basis through a GUI tool, to ensure that key systems are monitored as frequently as necessary. Where there are severe bandwidth problems, it should be possible for poll intervals to be changed to reduce network traffic.

1.1.11. The system shall support discriminated polling, whereby certain critical interface of routers or switches may be polled more frequently that others.

1.2. <u>Essential Requirements:</u>

1.2.1. NMS should have the ability to correlate events across the entire spectrum of infrastructure components that support our critical applications—routers. switched provided by heterogeneous vendors.

1.2.2. NMS architecture should be object-oriented, open, distributed, scalable, and multi-platform and open to third party integration.

1.2.3. The framework should be sensitive and be aware of the impact of management traffic on the network and provide mechanisms to limit use of network resources.

1.2.4. NMS should support ODBC Compliant database and interfaces to popular databases like SQL2005 Oracle, Ms.

1.2.5. NMS should quickly identify the impact of infrastructure failures (Identification of root cause of the problem) and manage the application services from business perspective.

1.2.6. The NMS should provide a robust event correlation engine.

1.2.7. System should be able to generate web-based reports.

1.2.8. NMS should support monitoring / managing of SNMP v1, v2c based devices.

1.2.9. NMS shall provide fault and performance management for multi-vendor TCP/IP networks.

1.2.10. The product should support dynamic object collections and auto discovery. The topology of the entire Network should be available in a single map.

1.2.11. NMS should provide accurate discovery of layer 3 and heterogeneous layer 2 switched networks for Ethernet and ATM, LANs and WANs.

1.2.12. The NMS should be able to discover redundant and ISDN Backup Links with proper color status propagation for complete network visualization.

1.2.13. Product should be able to update router configuration changes like re-indexing of ports, addition / deletion of ports on Network Map with each polling cycle without rediscovery of complete network / individual device.

1.2.14 The product should have web browser interface with user name and Password Authentication. It should be possible to view topology maps, events, reports etc. in full graphical format using standard web browser that support Java interfaces.

1.2.15. The product should support advanced filtering, to eliminate extraneous data / alarms.

1.2.16. The NMS shall support automatic event correlation, in order to reduce events occurring on such a large network, on events arising due to any of the following, Frame Relay, Cisco HSRP state. Pair Wise events (ex: link up/down) Chassis, Intermittent status, Node interface, Multiple reboot, De-duplication, Physical address mismatch, Authentication failure, Connector down. Scheduled maintenance.

1.2.17. The NMS should provide information regarding capacity utilization and error statistics for WAN links.

1.2.18. The NMS should trigger automated actions based on incoming events / traps

1.2.19. The NMS should be capable of login authentication to restrict / enable access to the manager.

1.2.20. NMS's event correlation shall be built-in, tightly coupled with NMS's event sub-system and should be able to suppress events for key systems/devices that are down for routine maintenance.

1.2.21. NMS shall have out of the box tools for building MIB Application used for testing devices on multiple MIB parameters. Data Collection should be possible on MIB Expressions using specific formulas like Utilization of Links in Kilo Bits Per Second, Mega Bits Per Second.

1.2.22. NMS shall have ability to display port labels on the connected devices on the network map. as configured in the routers. Ex: 64 kbps link from Safderjung to Datacenter

1.2.23. NMS shall provide internal built-in database as well as compatibility to Oracle or MSL SQL Database. In the regional centers the NMS shall be deployed with the inbuilt database.

1.2.24. NMS shall be configurable to suppress events for key systems/devices that are down for routine maintenance or planned outage.

1.2.25. NMS shall support correlation of layer 2 switched information in connector-down circuit, including trunks and meshes.

1.2.26. NMS should provide custom visual mapping of layer 2 and 3 devices, connectivity and relationships

1.2.27. NMS should ship with out-of-the-box correlators to enhance root-cause analysis and to significantly reduce the number of events operator receives.

1.2.28. NMS should provide inbuilt Correlation Composer Graphical User Interface (GUI), which enables users to tailor the event correlation behavior of the correlators that are shipped with product. No need of any special programming knowledge should be required.

1.3. Route Management

1.3.1.1. NMS Shall maximizes network availability and customer satisfaction by rapidly identifying and diagnosing IP routing faults.

1.3.1.2. It shall detect and isolate the root cause of layer 3 network instabilities and anomalies

1.3.1.3. It shall verify and alerts on changes to routing redundancy, preventing costly service outages

1.3.1.4. It shall monitor the routing protocols that direct the flow of traffic throughout the network, and construct the routers' view of the network, compute and display changes in routes and topology in real time.

1.3.1.5. It shall support the major service provider networks, monitoring multiple BGP connections to peer and customer networks, while analyzing full Internet routes.

1.3.1.6. It shall display detailed data about routing events—such as link status, link metrics and new prefixes to diagnose and troubleshoot problems.

1.3.1.7. It shall allow the operators to select a high-level view of the network topology showing the status of all routers and links, focus in on a specific area of the network, or view only specific types of routers, such as backbone routers.

16/9/20

1.3.1.8. Selecting any source/destination pair shall highlight the active route between the nodes, allowing operators to focus their attention on relevant devices and links when diagnosing problems.

1.3.2. It shall concurrently monitor and analyze complex IP networks that may have multiple routing protocols (OSPF, IS-IS, BGP) and may span multiple autonomous systems.

2. Network Performance Management

2.1.1. Performance management system should be centralized in headquarters.

2.1.2. Performance for Networks must monitor a wide range of network protocols and devices. Monitored elements include the following. frame relay, LAN/WAN management information base II (MIB-II) interfaces asynchronous transfer mode (ATM), MPLS routers device resources—CPU, memory, and buffers on devices.

2.1.3. Diagnose performance problems using recent and historical data.

2.1.4. Must identify over- and under-utilized links

2.1.5. Must identify how device resources are affecting network performance.

2.1.6. document current network performance for internal use and customer service level agreements (SLA)

2.1.7. Must provide intelligent insight into QOS and provide inputs to the QOS team

2.1.8. Performance for Networks must deliver reports based on IT SLA terms. The reports should customize easily, shall be provisioned to. sort data by site (offshore or onshore) or internal department. Further, login security should limit the information a user can see, such as specific customer data or department data.

2.1.9. The following performance reports should be produced

2.1.9.1. Executive Summary report that gives an overall view of a group of elements, showing volume and other important metrics for the technology being viewed.

2.1.9.2. Capacity Planning report that provides a view of under- and over-utilized elements.

2.1.9.3. Forecast Report that focuses on resources that are projected to become over-utilized in 90 days.

2.1.9.4. Hot Spot, quick view, and top ten reports that identify elements of possible concern by exceptions, degree of change, and other criteria

2.1.9.5. Service Level report that shows the elements with the worst availability and worst response time—the two leading metrics used to monitor SLAs.

2.1.10. It should be possible to put logo on reports and arrange or change tables and graphs to meet staff requirements

ANNEXURE 11

UPS SPECIFICATION

SPECIFICATION FOR LINE INTERACTIVE UPS SYSTEM

Specification	Requirements
Capacity	600 VA
Technology	PWM using MOSFET
MAINS MODE	
AC Input Voltage	140V to 260V
Frequency	47 to 53 Hz
AC Output voltage	200V to 250V (with AVR)
Input Frequency	Synchronize to mains frequency
INVERTER MODE	
Output Voltage	230V ± 5%
Output Frequency	50 Hz ± 0.5 Hz
Voltage Regulation	8% for entire battery range
Lower Power Factor	0.8
Over load capacity	110% for 10 Minutes.
Load capacity	600 VA/ 1KVA/ 1.5 KVA
Inverter efficiency	85% with full load rated capacity on computer load
Transfer time	< 6 ms.
Batter type	SMF
Back up time	30 Minutes
Recharge time	8 hours to 90% charged after full discharged
Battery Make	CSB/PANASONIC/EXIDE/YUASA
Cold start	YES
General compatible	YES
No load shutdown automatically	YES
PROTECTION	Short circuit, DC under/over voltage
Certification	ISO 9001 & 14001
Safety Certification	IEC / EMC Safety Certification
RS-232 C Interface computer interface.	
Input filters for Line Noise and Spikes	
Indications	Mains presence, main mode, battery charging, UPS mode, Battery low,

26|9|2006

SPECIFICATION FOR LINE INTERACTIVE UPS SYSTEM

Specification	Requirements
Capacity	2 KVA
Technology	PWM using MOSFET
MAINS MODE	
AC Input Voltage	140V to 260V
Frequency	47 to 53 Hz
AC Output voltage	200V to 250V (with AVR)
Input Frequency	Synchronize to mains frequency
INVERTER MODE	
Output Voltage	230V ± 5%
Output Frequency	50 Hz ± 0.5 Hz
Voltage Regulation	8% for entire battery range
Lower Power Factor	0.8
Over load capacity	110% for 10 Minutes.
Load capacity	2KVA
Inverter efficiency	85% with full load rated capacity on computer load
Transfer time	< 6 ms.
Batter type	SMF
Back up time	30 Minutes
Recharge time	8 hours to 90% charged after full discharged
Battery Make	
Cold start	YES
General compatible	YES
No load shutdown automatically	YES
Protection	Short circuit, DC under/over voltage
Certification	ISO 9001 & 14001
Safety Certification	IEC / EMC Safety Certification
RS-232 C Interface computer interface.	
Input filters for Line Noise and Spikes	
Indications	Mains presence, main mode, battery charging, UPS mode, Battery low.

2/9/08

ANNEXURE 'M'

DOT MATRIX PRINTER SPECIFICATION

- 300 cps @ Draft 12 cpi
- 360 cps @ High Speed Draft 12 cpi
- 200 KB Input Buffer
- 6000 POH - MTBF
- Metallic Side Frames
- Flat Tractors in the Printer
- Original + 3 copy capability with 0.32 paper thickness
- Print Head Life: 200 million dots per pin
- Hindi language printing capability as text

26/5/2020

ANNEXURE N

TECHNICAL SPECIFICATIONS FOR MULTI POINT VIDEO CONFERENCING UNIT

MCU should be of open standards and should support all end points manufactured by different manufacturers.

MCU should support 10/100 ethernet, ISDN PRI, IP-VPN networks etc.

The MCU should have the resources to be able to connect minimum 24 sites over IP @ 2 mbps with 30 fps. The MCU should support ISDN, IP and Internet endpoints in the same conference.

The MCU should be supplied with the required hardware and software that will allow at least 22 locations in a single conference. The system shall provide real time group Video-conferencing facility for video and/or audio and/or graphic presentation. The MCU should be able to adjust-itself for the participants coming on varying speed such as 128 kbps to 2 mbps. The system should be able to connect on IP at 2 Mbps bandwidth.

Application based Quality of Services reacting to packet loss, jitter, latency and Network congestion (Dynamic bandwidth allocation and IP precedence). There should be no appreciable change in voice or video or graphics between point-to-point and multi-point.

Should have a powerful management system to provide the power and flexibility required for both local and remote access and support. Management system should allow Administrator to control/configure/view the conference. Administrator to be able to move participants between the layouts of a conference or create sub-conferences for private conversations.. MCU should provide the power to the Administrator selectively drop endpoints that may not be authorized to participate on the conference.

MCU should be equipped with a GUI or web based console for management and administration. The administrator should be able to schedule and manage conferences in various combinations.

Open standards & interoperability:
The system should allow for audio, video and graphics transcoding at different frame rates, at different speed of connectivity with different resolutions. The system should permit compatibility between different audio and video coding algorithms. The system should allow various network protocols connectivity with one another. It should provide facilities for endpoints from different makes to participate and at different transfer rate & conference reliability. Should comply with the ITU Standards on Video Conferencing. The vendor should provide all necessary support to integrate end-points of any other make, in case of need.

MCU should be a non-PC hardware based, multi point conferencing unit.

PC / Software based/Windows based MCU is not acceptable.

It should have the following features -

ITU standards : H.323 version 4.0, SIP standards compliant
Video coding : H.261, H.263, H.263+, H.263++, H.264
Resolution: QCIF,CIF, 4CIF, VGA, SVGA, XGA

H.281 far end camera control
Audio coding support : G.728, G.711, G.722, G.722.1standards
Audio transcoding support : G.711, G.722, G.723, G.728 in the same conference

Network interface : Should have standard interface of 10/100 Mbps Ethernet (IP)
Bandwidth supported : Up to 24 sites at 2 mbps over IP networks

Video Display modes :
Support for voice activated and continuous presence (CP) mode conferences (CP conferences should not be software switched)

- Support for H.264 in CP mode conference with all 22 sites

- Support for video transcoding on all ports, with no limit on the no. of video algorithms

- Support for up to minimum 20 video layouts

- Support for continuous presence of 16 users on one screen
- Support for picture-in-picture
- Dynamic CP layout adjustment (MCU will choose for you the best video layout according to the number of participants in your conference). MCU should be able to adjust CP layout every time a participant joins in or drops out, with no empty window
- Support lecture mode and auto-rolling (auto-rolling time is configurable)
- Support change from any CP mode to any CP mode or CP mode to voice activated mode in an ongoing conference
- Activate speaker frame – locate the speaker in a CP layout (configurable option, and color of frame can be configurable)
- Auto blow up of speaker (participant video will be enlarged from small quadrant to big quadrant when speaking)

Conference speed capabilities :

- Support for both symmetric and asymmetric continuous presence mode conference
- Support for mixed rate conferences – all 22 sites connected at different speeds in the same conference along with transcoding
- There should be no limitation on the number of speeds at which sites can connect into one conference
-application based Quality of Services reacting to packet loss, jitter, latency and Network congestion (Dynamic bandwidth allocation and IP precedence). There should be no appreciable change in voice or video or graphics between point-to-point and multi-point.

Other conference features :
- Support minimum of 12 simultaneous CP conferences
- Full integration with Microsoft Office Live Communications Server (LCS) allowing multi point voice and video with Windows Messenger
- Support for H.235 Encryption (AES and DES).

- No loss in port capacity in an encrypted call up to 768 kbps
- Support text overlay for participant name display and also borders for active and displayed participant speaker Operator assistance available through using a GUI
Local View for Child Conference
- Allows operator in a cascaded conference to monitor its local conference, while local

26/9/2006

participants view the Master conference

- Intuitive and easy to use centralized web management

- Support for ISDN fallback for backup route when problem/overflow on the IP link and if the IP bandwidth is not available the call should made through the gateway and from the gateway to an IP on a different zone.

- The MCU should have the capability of supporting / integrating with other parties Video Conferencing Network.

Broadcast Mode:

All sites view the pre-assigned broadcaster
All sites should be muted centrally

Presentation mode

A single endpoint does a broadcast both video and live graphics PC presentation to all the endpoints.
End points must be allowed to raise questions/speak and accordingly image is to be switched.

Dual streaming support (dual video) using ITU-H.239 standards - support display both channels (data and video) of the presenter on the single CP layout screen. support lecture mode and CP change

Support cascading/clustering Support full web-based system configuration and conference control

IP based back-plane

Should have capability to connect to internal system
Support for ITU standards based packet loss compensation algorithm

Password protection

Web based Conference scheduling software supporting the following functionality :

Microsoft Outlook integration
Browser and Outlook based scheduling
E-mail notification to attendees of date, time and topic of conference
Conference templates for personalized and easy scheduling
Seamless conference control on one screen – dynamically add new participants. disconnect or reconnect endpoints, change screen layouts. extend conferences etc

- Ad hoc and scheduled meetings support
- Ability to pre-define conference layout, user position

External Gatekeeper for H.323 end points (VC/VoIP), registering with all endpoints with names and alias numbers and should operate in multiple IP zones. bandwidth management.

Should support the following features:

Standards supported : H.323 v4
Support for up to 50 users in the network at any point of time
Support for alias name, e.164 and IP address registration for H.323 users
Support IP address translation, user can make call using e.164 number
Monitors current number of on-call users
Monitors current number of online users
Monitors current used bandwidth
Support for bandwidth management - the gatekeeper must allow for the operator to initiate a call regardless of the end point used and independently of the availability of a bridge

Simplified dial plan
Inter-zone bandwidth management
Advanced PBX capabilities – H.450 call forwarding and transfer
Complete CDR for billing and accounting
Conference line and group hunting services
Simple fault monitoring
Third-party call control enabling instant initiation of multipoint conferences on-demand
Central configuration & management for multi-gatekeeper network.
Provide gatekeeper zone and neighbor gatekeeper features, for future expansion
Support call transfer and call forward functions
Provide web-based management interface with H.341 support that allows third party customization
Registration restrictions - define rules for specifying the length of the e.164 alias, the alias prefix and the range of IP addresses with which the gatekeeper allows an endpoint to register

Windows based OS required

Network Management software supporting the following functionality :

Network status updates – MCU elements, call, bandwidth, end point information, error status
Conference View – MCU controlling the conference, conference ID, conference type, video and bandwidth settings, number of participants – including the current no., the number reserved and the no. of local participants
Centralised log management – for network and element type levels, log files for MCU elements and gateways, that do not maintain their own log files
Should support SNMP based monitoring.

26|9|2006

ANNEXURE 'O'

TECHNICAL SPECIFICATIONS FOR GROUP CONFERENCING SYSTEM - CODEC & CAMERA DETACHABLE

Description	Requirements
Video Conferencing Protocols	ITU supported standards H.320 H.323 H.239
H.320 (ISDN)	Should support for ISDN – PRI network at later stage
H.323 (IP)	Should have Ethernet/IP interface up to 4 Mbps bandwidth
	Should support SIP protocol
Frame Rate	15 fps (frames per second) @ 56Kbps up to 128 Kbps 30 fps (frames per second) @ 256Kbps up to 2 Mbps
Network features	IP QoS: IP precedence/Diffserv, NAT, Packet loss recovery method
Video Standards	H.261, H.263 H263++ H.264, MPEG 4 Should support PAL standard
Video Input	PTZ (Pan Tilt Zoom) Camera Minimum 1 no S-Video / composite for Auxiliary Video Input or Document camera
Video Output	Main Monitor : S-Video/composite Dual Monitor : S-Video/Composite XGA / RGB output in codec for connecting projector/PC monitor
Audio Standards	G711 G.722 G.722.1 G.728 G.723.1 MPEG 4 AAC
Resolution	QCIF, FCIF CIF 4CIF 704 x 576 pixels for still images
Audio Input	Table Top mic input 2x Composite input 2x external mic input – phono type Should have support for additional microphone
Microphone	The microphone for the best sound quality and 360 degrees Omni directional coverage
Audio Output	1 Composite (RCA) line level for main Audio 1 Composite (RCA) line level (mixed audio out) for recording purpose
Features	Full duplex dynamic echo-cancellation Automatic gain control Automatic noise suppression

PTZ Camera	Detachable from CODEC With minimum of 240 degree Field of View Minimum 10X zoom Auto focus Automatic white balance Minimum 5 camera presets Far end Camera control
Ethernet/ Internet/ Intranet Connectivity	**Support for TCP/IP** 10/ 100 Mbps port (full duplex) Should be possible to configure port speed and mode
Multipoint calling capability **(Capability for Upgradation at a later date)**	End point should be capable of multipoint calling of minimum of four **(1+4)** remote sites over IP @ 512 kbps per site MCU Compatibility H.243 Compatible with analog and mobile networks Continuous presence video Should be able to display the site name during the call Should be possible to start the multipoint call from a point to point session, without creating the conference before
User Interfaces	Supports AMX or Creston touch panels Handheld Remote control and Web access mode
Security	Built-in encryption support for Video Call with AES Encryption H.235, H.233, H.234
Management & Other Features	Should be possible to access /manage the unit from a PC via LAN network Password protection for web access mode Should be able to see the calls record via web access mode in HTML format Should be possible to control the camera from web access interface Should be possible to stream out video from CODEC during point to point or multipoint session Should be possible to record a video session without using an external device like VCR or PC. System Should have built in recording facility

Other mandatory requirements

The Group Conferencing System quoted should be upgradeable for multi point capability as specified above without changing any of the components / model

16/9/14

PTZ Camera	Detachable from CODEC With minimum of 240 degree Field of View Minimum 10X zoom Auto focus Automatic white balance Minimum 5 camera presets Far end Camera control
Ethernet/ Internet/ Intranet Connectivity	**Support for TCP/IP** 10/ 100 Mbps port (full duplex) Should be possible to configure port speed and mode
Multipoint calling capability **(Capability for Upgradation at a later date)**	End point should be capable of multipoint calling of minimum of four (1+4) remote sites over IP @ 512 kbps per site MCU Compatibility H.243 Compatible with analog and mobile networks Continuous presence video Should be able to display the site name during the call Should be possible to start the multipoint call from a point to point session, without creating the conference before
User Interfaces	Supports AMX or Creston touch panels Handheld Remote control and Web access mode
Security	Built-in encryption support for Video Call with AES Encryption H.235, H.233, H.234
Management & Other Features	Should be possible to access /manage the unit from a PC via LAN network Password protection for web access mode Should be able to see the calls record via web access mode in HTML format Should be possible to control the camera from web access interface Should be possible to stream out video from CODEC during point to point or multipoint session Should be possible to record a video session without using an external device like VCR or PC. System Should have built in recording facility

Other mandatory requirements

The Group Conferencing System quoted should be upgradeable for multi point capability as specified above without changing any of the components / model

16\9\14

ANNEX [illegible]

TECHNICAL SPECIFICATION LINK ENCRYPTOR

Requirements

- Should be indigenously developed, field proven.
- The link encryptor so provided must have cover time for a period of 1 year for providing secrecy as required by the department. The same be approved by the competent body authorized by the Govt of India.
- Should work with data rates from 64Kbps up to 2mbps (64, 128, 256, 384, 448, 512, 768, 1024 and 2048 Kbps) to encrypt/decrypt for both voice and data in full duplex and synchronous operation.
- Should have Separate keys in transmit and receive directions.
- Should have Crypto data loading and code setting through Memory/Smart card.
- Should support password protection for crypto data loading and storage.
- Should have Keys loaded in flash memory.
- Should support automatic changing of keys at prescribe selectable times as well as manual changing.
- Reading/Changing by accident of stored or set codes should not be possible.
- Should have visual indication to indicate healthy and failure conditions.

Technical Specifications:

Crack resistivity	:	1 year
Scheme	:	Self synchronizing
Data rate	:	64 / 128 / 256 / 384 / 448 / 512 / 768 / 1024 & 2048Kbps
Type of application	:	Link encryption
Signaling	:	In secure mode as a part of bulk data
Traffic	:	In secure mode
Interface	:	Input -V.35 Output-V.35/ or G.703

28/9/10

Key management	:	Memory Card based
Packaging	:	19" rack mountable
Power supply	:	230V AC

Note- Vender should also mention about encryptor to be used for MPLS backbone. This should also be clarified that the same encryptor used with leased line configuration be also used for MPLS or otherwise.

(Kamalesh Deka)
Inspector General (Comn & IT)
BSF

Brig. M.K.Gupta 05 Nov 08
DIG (Communication)
NSG

Shri J.P.Sayal 3/x/2008
ADIG (IT)
BSF

Shri A.K.Gupta
Dy Director
DCPW

Shri S.K.Jindal
Scientist, 'F'
DRDO

3/11/08
Shri RakeshKumar
DD(QA), DGS&D