"शिक्षा स्वास्थ्य पर्यटन र व्यापारिक पूर्वाधार; बहुसाँस्कृतिक आवासीय समृद्ध सहर"

धरान उपमहानगरपालिका
DHARAN SUB-METROPOLITAN CITY
नगर कार्यपालिकाको कार्यालय
OFFICE OF THE MUNICIPAL EXECUTIVE

धरान, सुनसरी

Dharan, Sunsari

प.सं. २०८२/८३

च.नं. ६६४६

नेपाल संवत्: ११४६

मितिः २०८३/०१/२९

विषयः दरभाउ पत्र पेश गर्ने बारे सूचना ।

उपरोक्त विषयमा यस उपमहानगरपालिकालाई तपसिल बमोजिमका सामानहरुको आवश्यकता परेको हुँदा आजको मितिबाट बढीमा सात दिन भित्र दरभाउ पेश गर्न हुन यो सूचना सार्वजनिक गरिन्छ ।

तपसिल

S.N.	Budget heading	Qualification	Minimum Experience	Working Unit	Cost Per month (in NPR)	Cost Per day (in NPR)	Days	Total (NRS)
1	Project Manager	Master's degree in IT	5	1			13	
2	System Architect Analyst	Bachelor's in IT and relevant Certification	5	1			8	
3	System/Network Administrator	Bachelor's in IT with Network / System Certification	5	2			12	
4	Information Security Officer/ SOC Analyst (L2) / Incident Response Specialist	Bachelor's in IT with relevant certification	5	1			8	
5	Documentation Expert	Bachelors degree in any stream with good knowledge in ICT	2	1			3	
6	Support for this FY 2082/83	Network support and support for ISP change						
Total								
13% VAT								
Grand Total								

Dharan Sub Metropolitan City

Office of the Municipal Executive

Dharan

Terms of Reference (**TOR**) for

"Network Configuration, Segmentation & Monitoring of Dharan Sub-Metropolitan City"

Prepared By:

Dharan Sub Metropolitan City, Office of Municipal Executive

Dharan, Sunsari, Koshi Province

Terms of Reference (TOR)

अधिकृत सातौं

अधिकृतस्तर आठौं

तीर्थराज राई
प्रमुख प्रशासकीय अधिकृत

Table of Contents

नगर कार्यपालिकाको कार्यालय
धनगढी उपमहानगरपालिका
धनगढी-१२, सुदूरपश्चिम
कोशी प्रदेश, नेपाल

अधिकृतस्तर आठ

अधिकृत साताँ

अधिकृतस्तर आठौं

तीर्थराज राई
प्रमुख प्रशासकीय अधिकृत

1. Background

The office operates across **three floors** with approximately **30 rooms** and **100+ computers**, along with printers, IP devices, and wireless access points.
The organization has already procured the following networking equipment:

- Sophos Firewall
- 2 × Cisco 24-port Managed Switches
- 10 × 24-port Unmanaged Switches
- 3 × Wireless Access Points
- Server Rack (42U)
- Structured cabling and accessories

Currently, the network operates without proper segmentation, centralized monitoring, or bandwidth control. This results in:

- Flat network architecture
- Security risks
- Bandwidth misuse
- Lack of device visibility
- Difficult troubleshooting

Therefore, the office intends to **implement a secure, VLAN-based, centrally managed network architecture** with monitoring and documentation.

2. Objectives

The main objectives of this assignment are to:

1. Design and implement secure VLAN-based network segmentation
2. Allocate separate subnets for each section/department
3. Configure firewall policies for controlled access
4. Enable bandwidth management and traffic shaping
5. Implement centralized monitoring using PRTG
6. Improve network security, performance, and visibility
7. Provide proper documentation and knowledge transfer

3. Scope of Work

The selected service provider/consultant shall perform the following tasks:

3.1 Network Design

- Study existing infrastructure
- Prepare logical network diagram
- Prepare IP addressing plan
- Design VLAN architecture

3.2 VLAN & Subnet Segmentation

Separate VLANs/subnets for:

अधिकृतस्तर आ...

तीर्थराज राई
प्रमुख प्रशासकीय अधिकृत

- Administration
- Revenue
- Accounts and Audit
- Engineering and Planning Division
- Education Division
- Management
- IT Section
- Guest/Visitor Wi-Fi
- Access Points (Management VLAN)

Example:

VLAN	Section	Subnet
10	Admin	192.168.10.0/24
20	Finance	192.168.20.0/24
30	Social Development	192.168.30.0/24
40	Engineering	192.168.40.0/24
50	IT	192.168.50.0/24
60	Guest Wi-Fi	192.168.60.0/24
70	AP Management	192.168.70.0/24

3.3 Firewall Configuration (Sophos XGS 3100)

- *VLAN Interfaces Creation*

Logical interfaces shall be created on the firewall for each VLAN/department. Each interface will act as a gateway for its respective subnet, enabling proper routing, traffic control, and policy enforcement between networks.

- DHCP Configuration

Dynamic Host Configuration Protocol (DHCP) services shall be configured to automatically assign IP addresses, subnet masks, gateway, and DNS settings to client devices within each VLAN. This ensures simplified network management and avoids manual IP conflicts.

- *NAT Setup*

Network Address Translation (NAT) shall be configured to allow internal private IP addresses to securely access the internet through a public IP. NAT also hides internal network structure, improving security and efficient use of public IP resources.

अधिकृत साक्षी

अधिकृतस्तर आधि

तीर्थराज राई
प्रमुख प्रशासकीय अधिकृत

स्थानीय सरकार
धनगढी उपमहानगरपालिका
कार्यपालिकाको कार्यालय
धनगढी-१२, सुनसरी
कोशी प्रदेश, नेपाल

- Internet Policies

Firewall rules shall be defined to regulate internet access for different sections. Policies may include allowing or restricting specific services (web, email, downloads, social media, etc.), controlling usage time, and ensuring official work traffic is prioritized.

- *Inter-VLAN Security Rules*

Security rules shall be implemented to control communication between departments. Only authorized traffic will be allowed (e.g., IT access to all networks), while unnecessary or risky access (e.g., guest to internal LAN) will be blocked to enhance security and isolation.

- Bandwidth Control & QoS

Quality of Service (QoS) and bandwidth management policies shall be applied to allocate and prioritize network bandwidth. Critical services (official applications, video meetings, government portals) will receive higher priority, while non-essential traffic will be limited to prevent congestion.

- *Web Filtering (Optional)*

Content filtering may be enabled to block inappropriate or non-work-related websites such as social media, streaming, gambling, or malicious sites. This improves productivity and protects the network from cyber threats.

- Logging & Reporting

The firewall shall maintain detailed logs of network activity, user access, security events, and bandwidth usage. Periodic reports will be generated for monitoring, troubleshooting, auditing, and management review.

3.4 Managed Switch Configuration (Cisco)

- VLAN Creation

Virtual LANs (VLANs) shall be created on the managed switches to logically separate network traffic for different departments or sections. This segmentation improves security, reduces broadcast traffic, and enhances overall network performance and management.

- Trunk Configuration

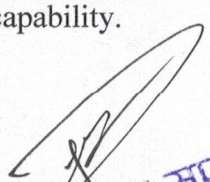
Trunk ports shall be configured between switches and the firewall to carry multiple VLANs over a single physical link. This enables interconnection of all VLANs across floors while maintaining proper segregation of network traffic.

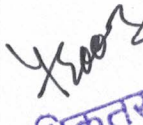
- Access Port Assignment

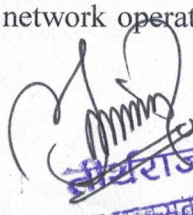
Individual switch ports shall be assigned as access ports and mapped to their respective VLANs. End-user devices such as computers, printers, and IP phones will connect through these ports, ensuring they receive the correct subnet and network policy.

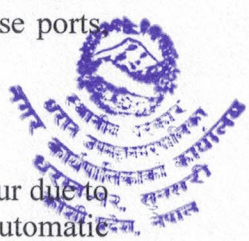
- STP/RSTP (Spanning Tree Protocol / Rapid Spanning Tree Protocol)

STP/RSTP shall be enabled to prevent network loops and broadcast storms that may occur due to redundant links. This ensures stable, reliable, and continuous network operation with automatic failover capability.









- Basic Security Hardening

Security best practices shall be implemented, including disabling unused ports, setting strong administrative passwords, restricting unauthorized access, enabling port security, and protecting management interfaces to safeguard the network from internal and external threats.

- Port Labeling

All switch ports shall be properly labeled and documented according to their connected devices or departments. This facilitates easier troubleshooting, maintenance, and future expansion of the network.

3.5 Wireless Network Setup

- Configure APs

All installed Wireless Access Points shall be logically configured to provide reliable and uniform wireless coverage across all floors and rooms. Proper placement, channel selection, and power adjustment shall be carried out to minimize interference and ensure stable connectivity.

- Separate SSIDs

Multiple Service Set Identifiers (SSIDs) shall be created to logically separate different categories of wireless users (e.g., staff and guests). This ensures controlled access, improved security, and easier network management.

- Staff Network

A secure wireless network shall be configured for office staff with authentication and access to internal resources such as servers, printers, and applications. This network will follow organizational security policies and may include password or enterprise authentication.

- Guest Network (Internet Only)

A separate guest Wi-Fi network shall be established exclusively for visitors. This network will provide internet access only and will be isolated from internal LAN resources to prevent unauthorized access and enhance security.

- VLAN Tagging

Wireless traffic shall be mapped to corresponding VLANs through VLAN tagging. This ensures that staff, guest, and management traffic remain logically separated and follow the same security and routing policies as the wired network.

3.6 Network Monitoring (NAGIOS)

- Install & Configure NAGIOS

The NAGIOS monitoring system shall be installed and properly configured on a designated server to provide centralized monitoring of all critical network devices and services. System settings, dashboards, and user access controls shall be established for efficient administration.

अधिकृतस्तर आ०
तीर्थराज राई
प्रमुख प्रशासकीय अधिकृत
कार्यपालिकाको कार्यालय

- Device Discovery

Automatic and manual discovery methods shall be used to identify and register all network-connected devices such as firewall, switches, access points, and servers. This ensures complete visibility and inclusion of all assets in the monitoring system.

- Add Sensors for Devices

o Firewall

Monitoring checks shall be configured for firewall availability, CPU/memory usage, interface status, session count, and internet connectivity to ensure continuous security and gateway performance.

o Switches

Switch monitoring shall include device uptime, port status, traffic utilization, errors, and hardware health to detect failures or congestion in the internal network.

o APs (Access Points)

Wireless devices shall be monitored for availability, connected clients, signal performance, and traffic usage to ensure consistent wireless service quality.

o Bandwidth Usage

Bandwidth utilization sensors shall track incoming and outgoing traffic across critical links to analyze consumption patterns, detect misuse, and support bandwidth management and capacity planning.

- Alerts & Reports

The system shall generate real-time alerts via email/SMS/dashboard notifications for device failures or threshold breaches. Periodic reports (daily/weekly/monthly) shall be produced to summarize uptime, performance, and bandwidth usage for management review and audit purposes.

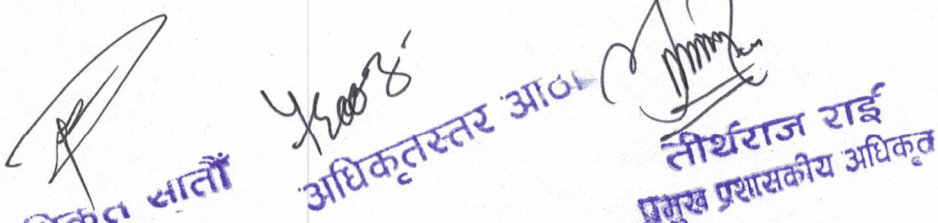
3.7 Testing & Optimization

- Connectivity Testing

All network components including firewall, switches, access points, servers, and end-user devices shall be tested to verify proper connectivity within each VLAN and controlled communication between VLANs. Internet access, internal resource access, and device reachability shall be confirmed to ensure the network is functioning as designed.

- Throughput Testing

Network performance tests shall be conducted to measure bandwidth, speed, latency, and data transfer rates across wired and wireless segments. This ensures that the infrastructure meets operational requirements and identifies any bottlenecks or congestion that may affect productivity.



- Security Verification

Security checks shall be performed to validate firewall rules, VLAN isolation, access restrictions, and guest network separation. Unauthorized access attempts shall be tested to confirm that internal resources are protected and that the network complies with security policies.

- Failover Testing

Redundancy and recovery mechanisms shall be tested by simulating device or link failures. The network shall automatically recover or reroute traffic with minimal downtime to ensure business continuity and reliable service availability.

3.8 Documentation & Training

- SOP
- Network diagram
- Configuration backup
- Admin training

4. Deliverables

The consultant/vendor shall submit:

1. Network Design Document
2. VLAN & IP Addressing Plan
3. Configured Firewall
4. Configured Switches
5. Configured Wi-Fi
6. NAGIOS Monitoring Setup
7. Logical Network Diagram (PDF)
8. Firewall Rule Matrix
9. Configuration Backup Files
10. Handover & Training Report

5. Timeline

Phase	Activity	Duration
Phase 1	Site Study & Network Design	Day 1–5
Phase 2	Firewall & Switch Configuration	Day 4–9
Phase 3	Wi-Fi setup	Day 8–10
Phase 4	Network Monitoring Setup	Day 9–13
Phase 5	Testing & optimization	Day 12–15

अधिकृतस्तर आठ।

सार्थराज राई

Phase	Activity	Duration
Phase 6	Documentation	Day 14–16
Phase 7	Buffer & Final Handover	Day 17–22
Total		**22 working days**

Role	Active Days
Project Manager	Day 1–5, 14–22
System Architect	Day 1–9
Network Admin (2)	Day 4–12
Security Officer	Day 9–15
Documentation Expert	Day 14–16

6. Acceptance Criteria

Work shall be considered complete when:

- All VLANs functional
- Internet accessible as per policy
- Guest isolated
- Monitoring operational
- Bandwidth control working
- Documents submitted

7. Reporting & Coordination

The consultant shall coordinate with:

- IT Section
- Network Administrator

8. Warranty / Support

- Minimum 3 months post-implementation support
- Remote troubleshooting
- Configuration assistance

अधिकृत सातौं

अधिकृतस्तर आठौं

तीर्थराज राई
प्रमुख प्रशासकीय अधिकृत