Organization Name:	GovTech Agency, Thimphu: Bhutan
Document Name:	Standard Operating Procedure for Incident & Problem Management
Document No:	GovTech/GovNets-01/(02)/2023-24
Version:	1.0
Effective Date:	**Jan 1, 2024**

Preparation, Review & Approval of the Document

Prepared by:	GovNets Division, Thimphu 1. Karma, Chief 2. Pema Dhendup, Dy.chief ICTO 3. Karma Jamyang, Dy.Chief ICTO 4. Karma Tenzin, ICT analyst 5. Rinchen Khando, Executive Engineer 6. Tashi Delek, ICTO 7. Sonam Tshering, ICTO 8. Mohan Kumar Pradhan, Sr.ICTA 9. Tshering Wangchuk, Sr.ICTA 10. Jigme Choda, Sr.ICTA 11. Sonam Dorji, ICT.TA II 12. Dendup Pema, ICT.TA II 13. Ugyen Tshomo, AICTO 14. Sonam Choden, AICTO 15. Tshering Dekar, AICTO 16. Sonam Choki, AICTO
Reviewed & Approved by:	Director, DDI GovTech Agency, Thimphu: Bhutan

Table of Content

Document Version History

Version	Date	Author	Description of Change

Terminology

Term	Description
GovNet	Government Networks
DrukREN	Druk Research and Education Network
Customer Premises Equipment (CPE)	Network equipment is placed at agencies that interface between access and internal networks.
Core Team	A team based in Head Quarter with the technical expertise to manage and operate both GovNet and DrukREN core networks.
Access Team	A team based either in the dzongkhags whose line of reporting is to the regional head or ICT sections based in agencies other than GovTech Agency within Thimphu.
RCA(Root Cause Analysis)	Investigation step within problem management that analyzes a problem to identify the root cause.
End-User	All the GovNet and DrukREN users
Recurring incident	The same incident was observed more than two times in the same segment of networks over a period of a month.
Network Monitoring System (NMS)	A Network Monitoring System is used to track the status of devices, alert users when predefined thresholds are exceeded, and analyze traffic.

Incident	Single unplanned issue that causes a network service disruption.
Problem	Recurring incidents more than one that causes a network service disruption.

1. Introduction

1.1 Purpose

This Standard Operating Procedure (SOP) defines the procedures for identifying, analyzing, and resolving problems with government networks (GovNet and DrukREN) to minimize the impact of incidents and prevent recurrence. The goal is to ensure the stability of network operations and improve service delivery through effective problem management. More importantly, it defines the roles and responsibilities of the concerned teams to resolve the issues effectively. This SOP was developed under the guidance and supervision of Mr. Stephen, a consultant for the GovTech agency. This SOP is intended to be read in conjunction with Request Fulfillment SOP.

The Government Network Division is mandated to maintain uptime as follows to provide reliable connectivity;

1. Core network uptime: 99.8%
   The core network constitutes both DrukREN and GovNet core network infrastructure such as fiber optical cables, core routers, gateway routers, border routers, and repeater switches, servers. *(Network Diagram -Annexure:1(A) & Annexure:1(B))*

2. Access network uptime:85 %
   The access network constitutes both DrukREN and GovNet access network infrastructure such as fiber optical cables, agency routers, core switches, Customer Premises Equipment (CPE), distribution switches *(Network Diagram-Annexure-2(A) & Annexure-2(B))*

3. Internal network uptime: 80%
   The internal network constitutes both DrukREN and GovNet internal network infrastructure such as layer 1 infrastructure, internal distribution switches, access points, the host computer *(Network Diagram-Annexure-3(A) & Annexure-3(B))*

1.2 Scope

This Standard Operating Procedure(SOP) is targeted to all the Network engineers and System Administrators for all the agencies connected to government networks (GovNet and

DrukREN). This SOP applies to all network-related problems, including recurring incidents, root cause analysis, and corrective action plans. It covers all the networking infrastructure including dzongkhag agency routers, gewog agency routers, dzongkhag CSW, gewog CSW, agencies CPE, access points, and host computers, with the exception of a few agencies listed in *Annexure 4*.

The procedure also covers configuration, security protocols, network management and monitoring tools, troubleshooting, and maintenance.

2. Roles and Responsibilities

Problem Management Team	
Core Team:	1. The Chief of Division will facilitate the root cause analysis sessions. 2. Troubleshoot and resolves the core network-related issues; 3. Resolve network-related issues that have escalated from the agencies based on their priorities(low, medium, high).
Access Team:	1. The respective Regional Head/Agency ICT officials will facilitate the root cause analysis sessions. 2. Troubleshoot and resolve access network-related issues; 3. Maintain documentation and troubleshooting reports; 4. Log downtime of the network; 5. Escalate the issues as per the Escalation Matrix for unresolved issues;
Fiber Team:	1. For nationalized fiber issues, DoTS teams under the supervision of the chief will be responsible to facilitate Root Cause Analysis sessions in coordination with the Fiber Network Division team assigned by BPC in the respective regions. 2. For non-nationalized fiber issues, the regional head will facilitate the root cause analysis in coordination with the identified ISPs in the respective regions.
System	1. For DNS issues, the GovNet system admin team

Administration Team:	facilitates coordination with the GDC team. 2. For system issues, the GovNet team facilitates coordination with the DSOM team. 3. For the ePIS system issue GovNet team to facilitate in coordination with the ePIS team.
Network Security Team:	1. For cyber threats(hacking, malware, phishing, and ransomware) GovNet Network Security team to facilitate coordination BtCRT team. 2. Unauthorized IP scanning

3. Identification and Classification of Problem

1. Gather information from end-users or through Network Monitoring tools.
2. Classify the issues as per the Impact and Urgency Matrix

Impact/Urgency	High	Medium	Low
High	P1(Critical)	P2(High)	P3(Medium)
Medium	P2(High)	P3(Medium)	P4(Low)
Low	P3(Medium)	P4(Low)	P4(Low)

P1(Critical): Affects entire network services in the whole agency;
P2(High): Affects major offices within the agency;
P3(Medium): Affects some network services of a few users;
P4(Low): Does not have a significant effect;

3.1 Problem Response Time ;

P1 (Critical): 5 to 10 minutes
P2 (High): 10 to 20 minutes
P3 (Medium): 30 to 40 minutes
P4 (Low): 1 to 2 hours

4. Root Cause Analysis (RCA) and Process Solution

Conduct RCA Using the Process of Elimination. Use the process of elimination to determine the root cause. Gather the members of the RCA team together to brainstorm a list of potential causes.

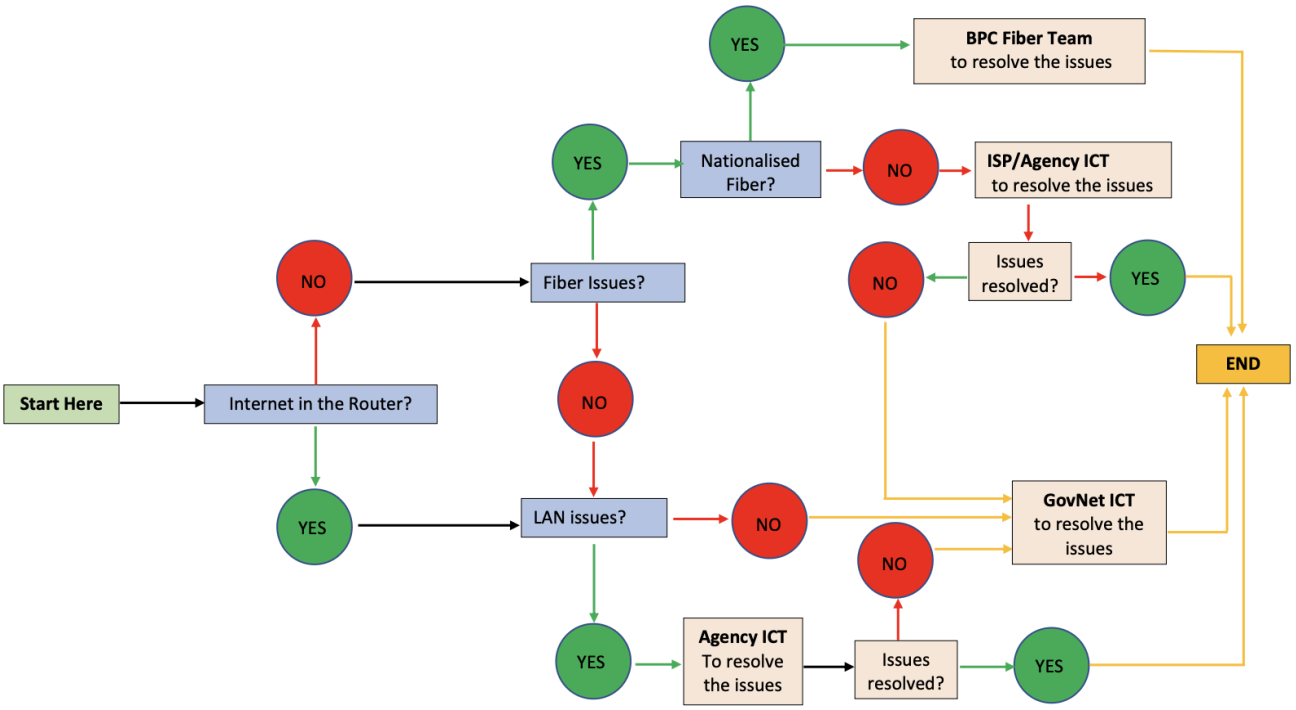


Fig1.0 Escalation Flow Diagram

4. 1.1 Internet in the Router?

4.1.2 Internet in Dzongkhag/Thromde or Agency Router - No

1. Check to ensure the router is powered on;
2. Check to ensure no physical damage to the router;
3. Check to ensure the link from the core router is active;
   3.1 Physical link LED status
   3.2 Run the command to check interface status;

For Cisco ios XE

Router#show interface descriptions
Interface Status Protocol Description
Gi0/0/0 up up Link from core-router

Both status and protocol should be up

For juniper JUNOS Base OS

Router> show interfaces descriptions
Interface Admin Link Description
xe-0/0/1 up up link to core-router

Both admin and link should be up

3.3 Run the command to check Rx optical transceiver status

For Cisco IOS-XE

***Router**#show hw-module subslot 0/0 transceiver 0 transceiver*
OR
***Router**#show hw-module interface Te0/0/0 transceiver transceiver*
Transceiver Rx optical power = -14.4 dBm

Transceiver Rx optical power should be within the threshold

For JUNOS Base OS

Switch-Ex4600> show interfaces diagnostics optics xe-0/0/0
Laser receiver power: 0.0138 mW / -18.60 dBm

Laser receiver power should be within the threshold

3.4 Use OTDR to check Rx power and fiber bend or breakage

4. Check to ensure the optical transceiver and fiber patch cord connecting to the agency routers are working fine;
   4.1 Run optical transceiver loopback testing and use Optical Power Meter (OPM) to check Tx Optical Power;
   4.2 Use OTDR to pass the laser through the fiber patch cord;

5. Check Router configurations
   5.1 Run the command to check the router configuration and ensure it is rightly configured as per the template Annexure(A)&(B)

4.1.3 Fiber Issues

OTDR to check and ensure bend and fiber breakage. The access team will determine whether it is nationalized or non-nationalized fiber

- **Nationalised Fiber Issues:** Raise the ticket to BPC via link https://fnd.bpc.bt/open.php and inform the core team and Division of Telecom and Space (DoTS)
- **Non-Nationalised Fiber Issues:** Coordinate with respective ISPs to resolve the issues; ISP details attached details *Annexure-9*

4.1.4 Internet in Dzongkhag/Thromde/Gewog/Autonomous Agency core switch- Yes

1. Proceed to troubleshoot the Local Area Network (LAN)

4.1.5 Local Area Network (LAN) Issues

4.1.5.1 Internet in Dzongkhag or Gewog Core Switch - No

1. Check to ensure the switch is powered on;
2. Check to ensure no physical damage to the switch;
3. Check to ensure the link from the core router is active;
   3.1 Physical link LED status
   3.2 Run the command to check interface status;

Cisco
Switch#show interface descriptions
Interface Status Protocol Description
Gi0/0/0 up up Link from agency-router
Both status and protocol should be up

Juniper Ex4300 Junos OS
Switch> show interfaces descriptions
Interface Admin Link Description
ge-0/0/1 up up link to Dechencholing Higher School

Both admin and link should be up

3.3 Run the command to check Rx optical transceiver status
3.4 Use OTDR to check Rx power and fiber bend or breakage;

4. Check to ensure the optical transceiver and fiber patch cord connecting to the core switch are working fine;
   4.1 Run optical transceiver loopback testing and use Optical Power Meter (OPM) to check Tx Optical Power;

   4.2 Use OTDR to pass the laser through the fiber patch cord;

5. Check Switch configurations
   5.1 Run the command to check the switch configuration and ensure it is rightly configured as per the template *(Annexure - 6(A) & Annexure - 6(B)*

- Escalate unresolved issues to the core team along with troubleshooting reports as per the formatAnnexure-7. Contact details of core team members are attached as Annexure-7

5. Problem Management Procedure

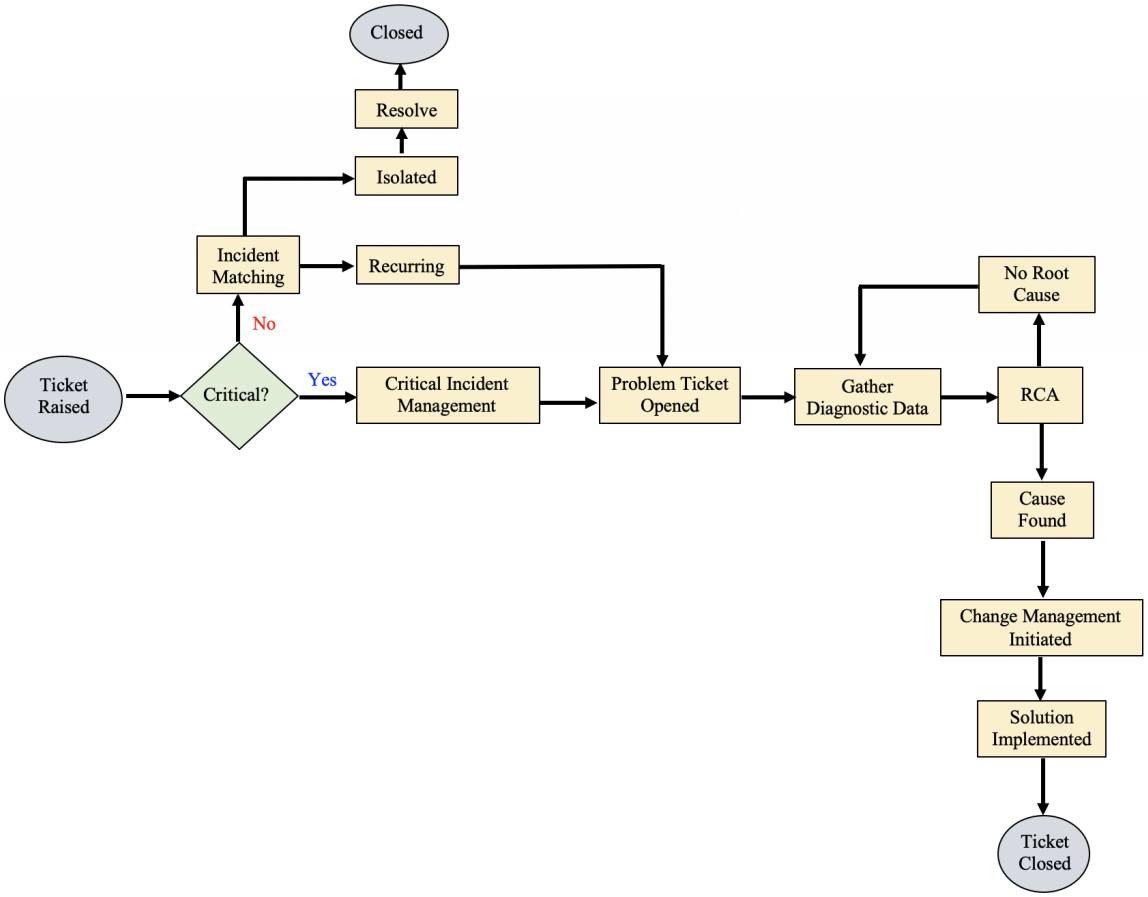


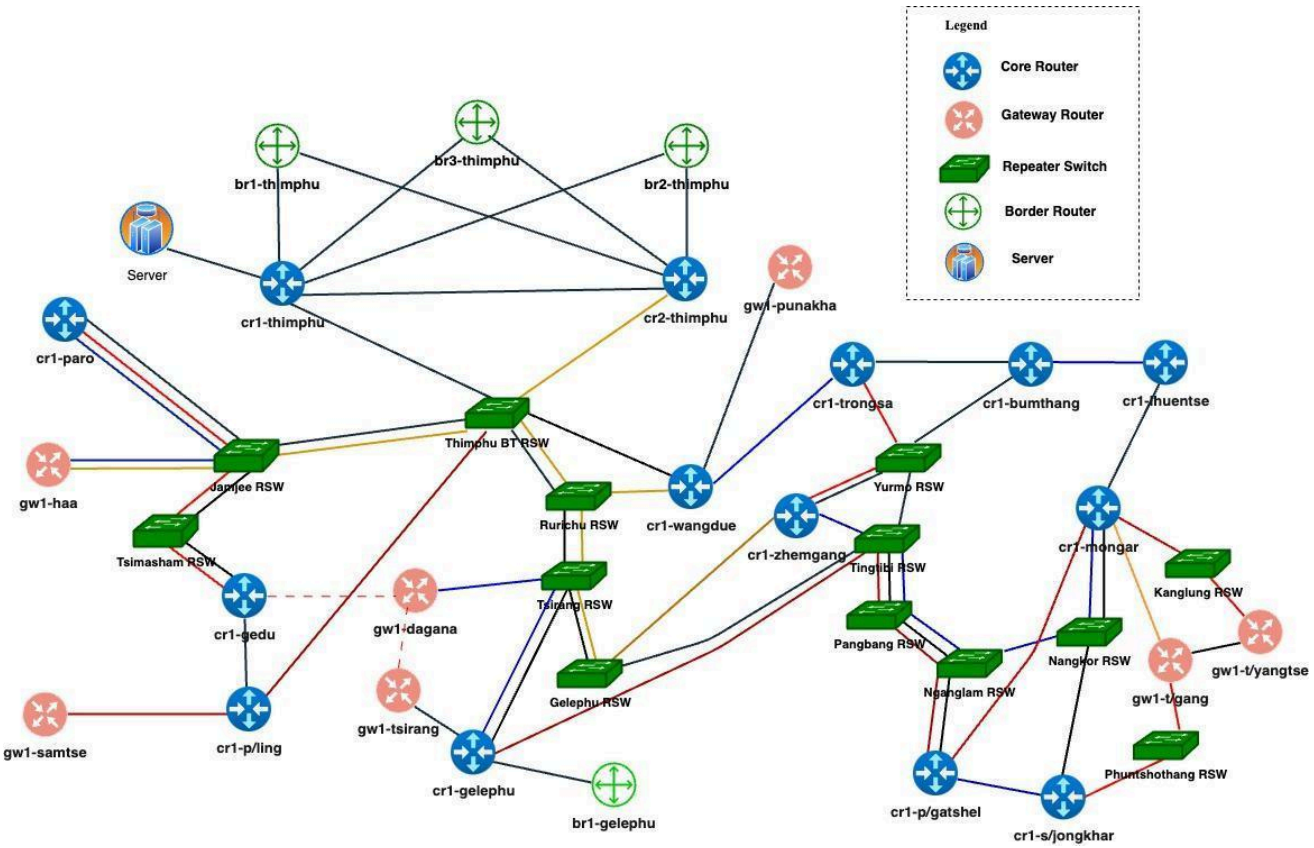
Fig1.1: Incident Management Flow Chart

5.1 Management of Problems using Ticketing System/Help Desk System(HDS)

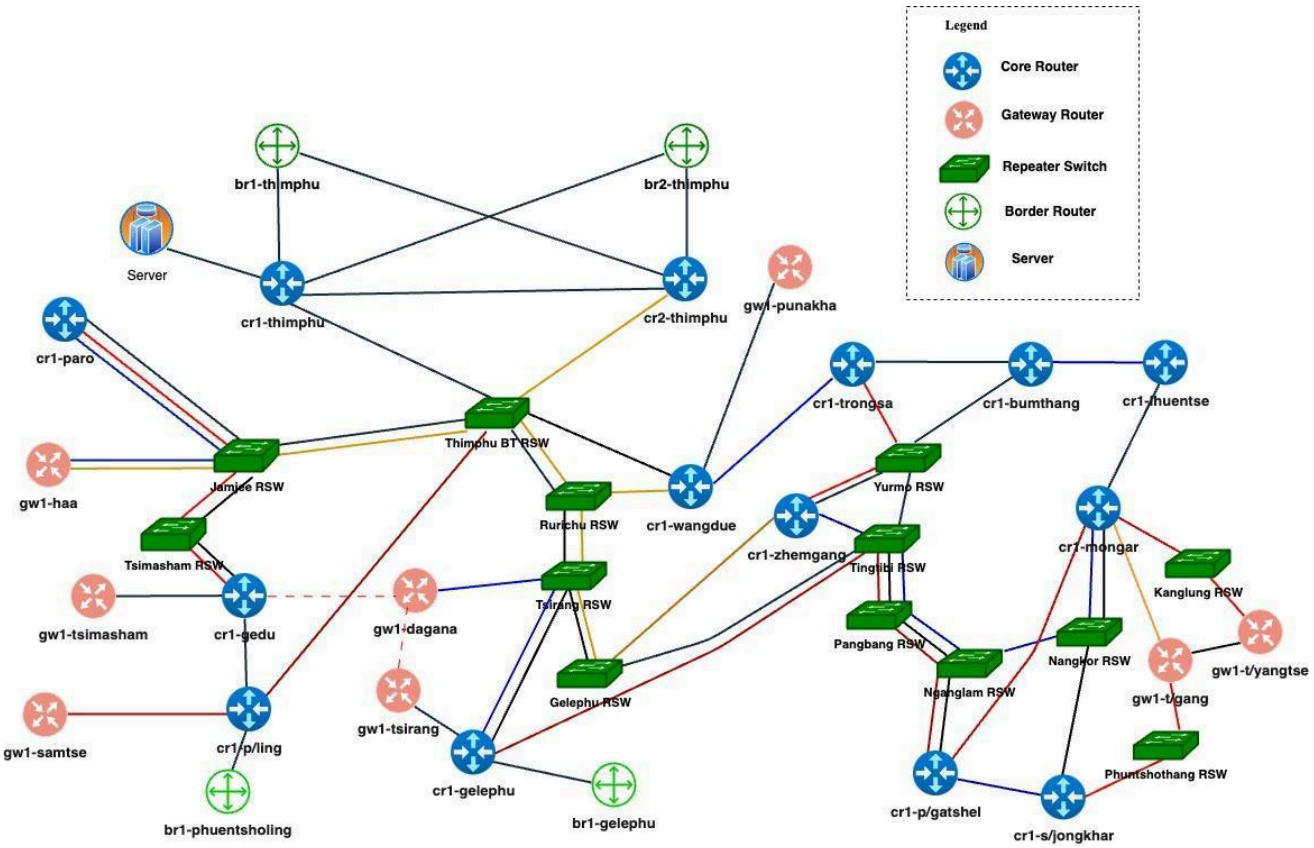
1. The end-user raises a ticket for the network-related incident through the system;
2. Based on the classification matrix, the ticket shall be identified as a critical or non-critical incident (s). The incident handler, while referring to the incident records, shall further classify the reported incident as recurring or isolated incidents for non-critical incidents.
3. The isolated incidents shall be resolved, and subsequently close the tickets.
4. The recurring incidents shall be treated as problems and process with the opening of tickets;
5. The problem ticket shall be classified and prioritized as per the Impact and Urgency Matrix mentioned in section 5;
6. The critical incidents shall proceed to critical incident management followed by opening the problem tickets;

7. Gather the diagnostic data and evidence from NMS, system logs, and other relevant tools;
8. The Problem Management Team shall conduct RCA and determine the root cause;
9. After identifying the root cause and solution, the team shall seek consensus and endorsement to implement the solution as part of change management process;
10. Implement the solution to resolve the issues.
11. Closed the ticket.
12. If the problem management team is unable to identify a root cause, the team should restart the RCA process following from step 7.
13. Note: In case the ticketing system is down, Google Forms can be used as an alternative solution

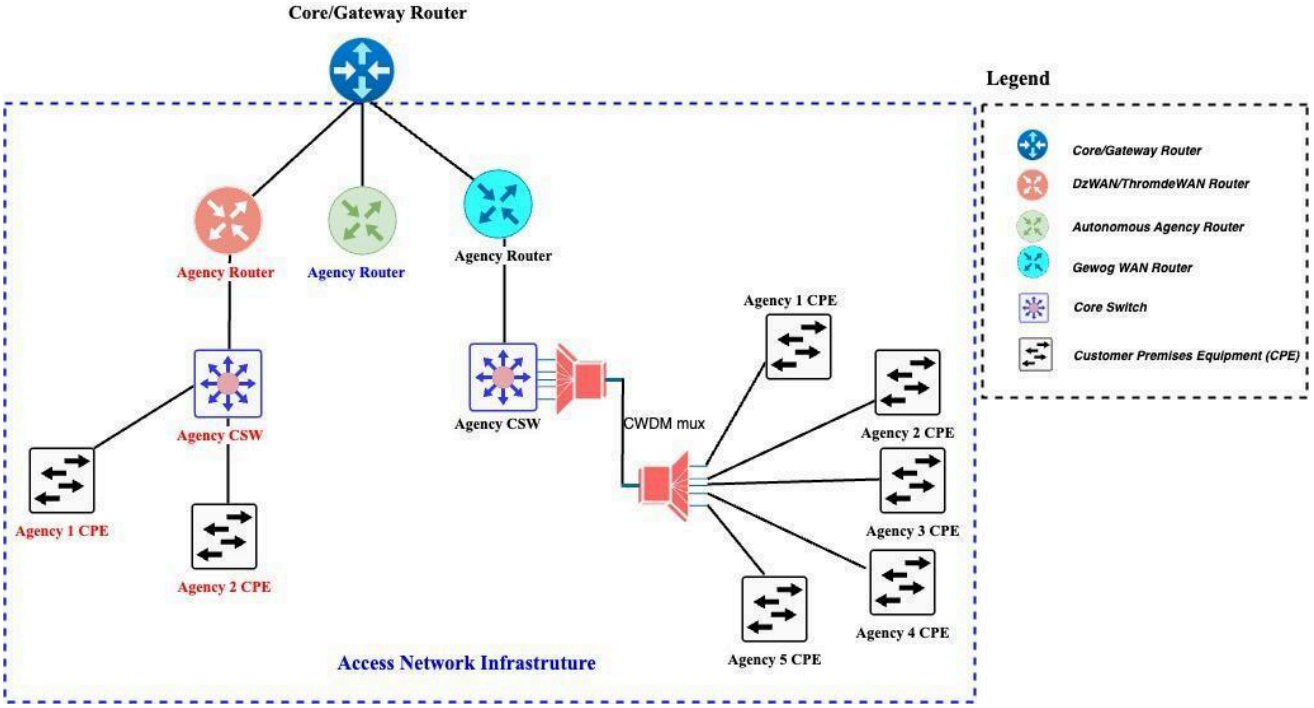
Annexure 1(A): GovNet Core Network Diagram



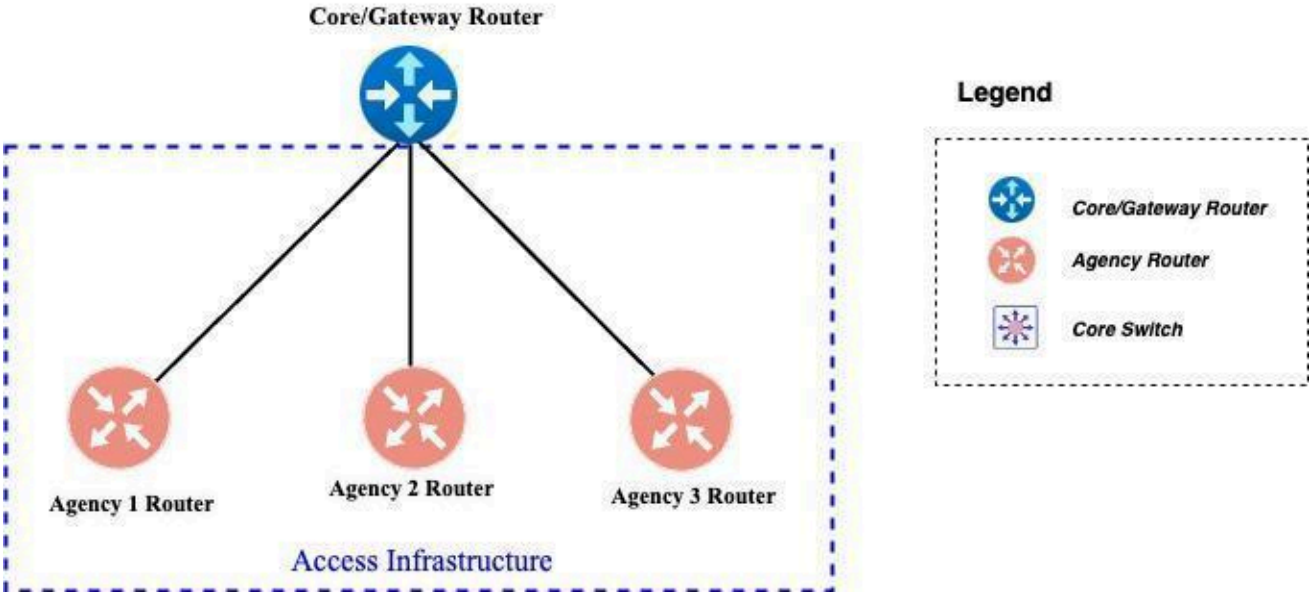
Annexure 1(B): DrukREN Core Network Diagram



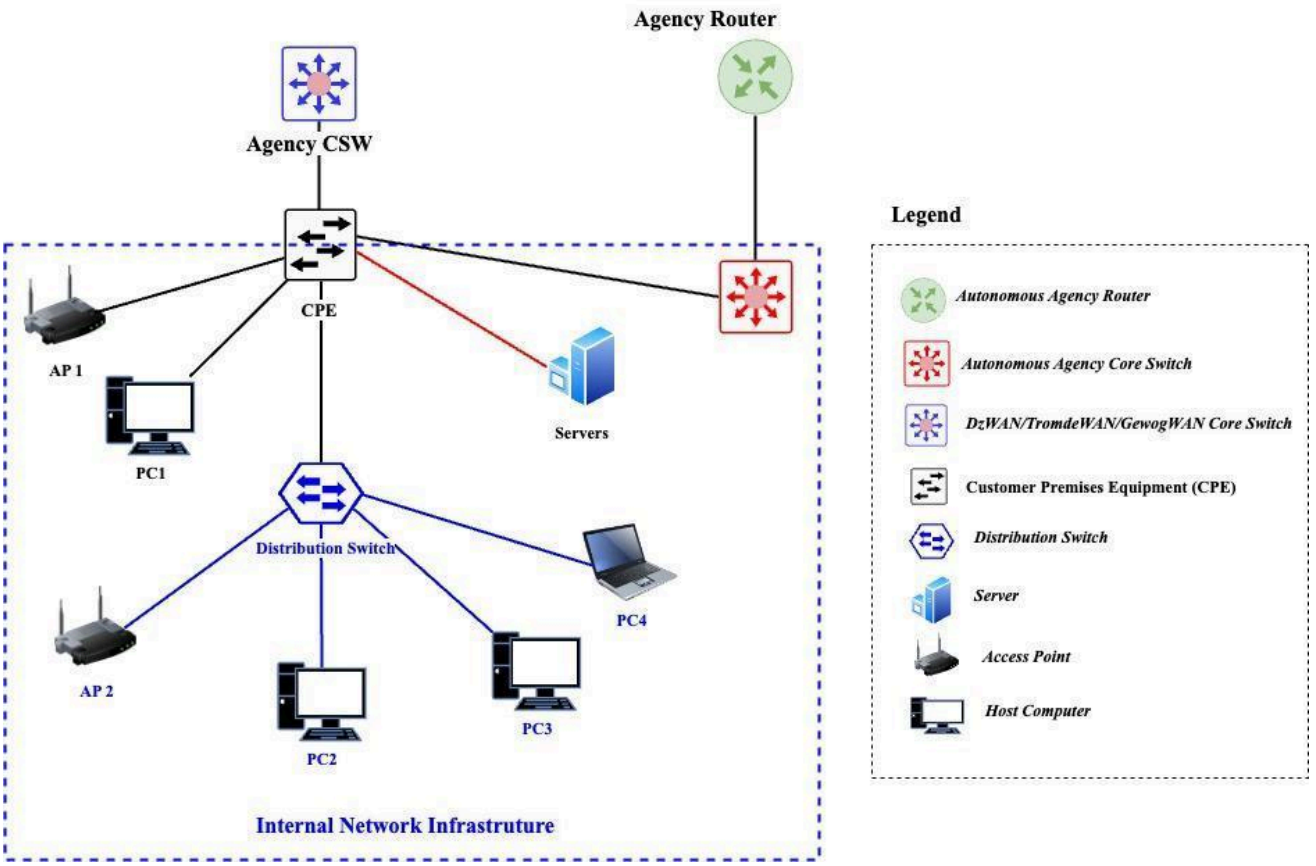
Annexure 2(A): GovNet Access Network Diagram



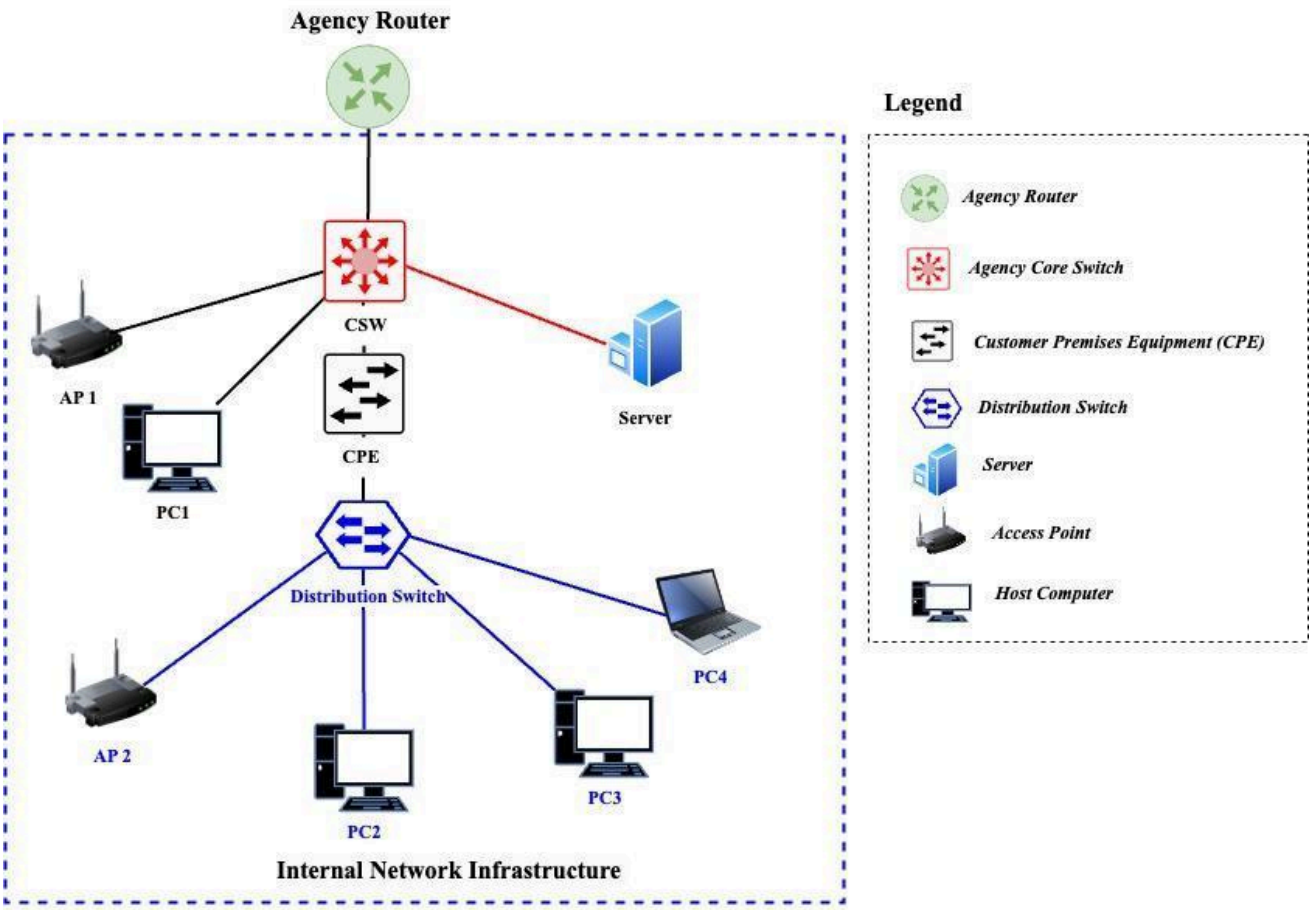
Annexure 2(B): DrukREN Access Network Diagram



Annexure 3(A): GovNet Internal Network Diagram



Annexure 3(B): DrukREN Internal Network Diagram



DrukREN Internal Network Diagram

Annexure IV - List of agencies that manage access and internal LAN independently

SN	Dzongkhag	Name of the Agency
1	Chhukha	Gedu College of Business Studies
2		College of Science and Technology
3	Paro	Paro College of Education
4		Jigme Singye Wangchuck Law School
5	Punakha	College of Natural Resources
6	Samdrup Jongkhar	Jigme Namgyel Engineering College
7	Samtse	Samtse College of Education
8	Thimphu	Office of Vice Chancellor, RUB
9		Khesar Gyalpo University of Medical Science
10		Faculty for Traditional Medicine
11		Gyalpozhing College of Information Technology,Chamina
12		Jigme Dorji Wangchuck National Referral Hospital (JDWNRH)
13		Faculty for Nursing & Public Health
14		Royal Thimphu College (RTC)
15		National Traditional Medicine Hospital (NTMH)
16	Trashigang	Sherubtse College
17		Yongphula Centenary College
18	Trongsa	College of Culture and Language Studies

Annexure 5(A) - GovNet Agency Router Configuration Template

*******Interface connecting to Core Router*******
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# description link to core router
Router(config-if)# ip address *x.x.x.x y.y.y.y*
Router(config-if)# ip nat outside
(x.x.x.x – p2p ipv4 address)
(y.y.y.y – subnet mask)

*******Interface connecting to Agency Core Switch*******
Router(config)# interface GigabitEthernet0/0/1
Router(config-if)# description link to core switch
Router(config-if)# ip address *x.x.x.x y.y.y.y*
Router(config-if)# ip nat inside
(x.x.x.x – p2p ipv4 address)
(y.y.y.y – subnet mask)

*******Management Interface******
Router(config)# interface GigabitEthernet0
Router(config-if)# description for management
Router(config-if)# ip address *x.x.x.x y.y.y.y*
(x.x.x.x – management ipv4 address)
(y.y.y.y – subnet mask)

******* eBGP with Core Router *******
Router(config)# router bgp *ASN*
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# bgp deterministic-med
Router(config-router)# timers bgp 15 45
Router(config-router)# neighbor *x.x.x.x* remote-as *152317*
Router(config-router)# neighbor *x.x.x.x* description ebgp with Core Router
Router(config-router)# neighbor *x.x.x.x* password *(Pasword)*
Router(config-router)# address-family ipv4
Router(config-router-af)# network *z.z.z.z* mask *y.y.y.y*
Router(config-router-af)# distance bgp 200 200 200
(*ASN – Private Autonomous System Number-Annexure-5.1(A)*)
(*x.x.x.x – core router p2p ipv4)*
(*152317 – Core Router Autonomous System Number)*
(*Pasword – BGP password - Annexure-5.1(A))*
(z.z.z.z – private ipv4 address allocated for agency)
(y.y.y.y – subnet mask)

******* Network Address Translation (NAT) *******

Router(config)# ip nat pool *pool-name x.x.x.x y.y.y.y.y prefix-length 30*
Router(config)# ip nat inside source list *pool-list* pool *pool-name* overload

Router(config)# ip access-list extended *pool-list*
Router(config)# 10 deny ip any 10.0.0.0 0.255.255.255
Router(config)# 20 deny ip any 172.16.0.0 0.15.255.255
Router(config)# 30 deny ip any 192.168.0.0 0.0.255.255
Router(config)# 40 deny ip any 157.10.120.0 0.0.3.255
Router(config)# 50 deny ip any 157.10.128.0 0.0.1.255
Router(config)# 60 deny ip any 157.10.136.0 0.0.7.255
Router(config)# 70 deny ip any 157.10.144.0 0.0.3.255
Router(config)# 80 permit ip *a.a.a.a. b.b.b.b* any
(pool-name – NAT pool name)
(pool-list – NAT pool list)
(30 – prefix-length 30 for subnet (/30))
(a.a.a.a – private ipv4 address allocated for agency)
(b.b.b.b – wildcard mask)

******* Default route configuration *******

Router(config)# ip route 0.0.0.0 0.0.0.0 *x.x.x.x* permanent
(x.x.x.x – core router p2p ipv4 address (next-hop))

******* Static route configuration *******

Router(config)# ip route *x.x.x.x y.y.y.y* z.z.z.z
(x.x.x.x – allocated private ipv4 address)
(y.y.y.y – subnet mask)
(z.z.z.z – core switch p2p ipv4 (next-hop))

Annexure 5(B) - DruREN Agency Router Configuration Template

*******Interface connecting to Core Router*******
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# description link to core router
Router(config-if)# ip address *x.x.x.x y.y.y.y*
Router(config-if)# ip nat outside
(x.x.x.x – p2p ipv4 address)
(y.y.y.y – subnet mask)

*******Link Aggregation Control Protocol (**Gi0/0/0 & Gi0/0/0)*****
Router(config)# interface Port-channel1
Router(config-if)# description link to core switch
Router(config-if)# no ip address

Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# description link to core switch
Router(config-if)# no ip address
Router(config-if)#channel-group 1 mode active

Router(config)# interface GigabitEthernet0/0/1
Router(config-if)# description link to core switch
Router(config-if)# no ip address
Router(config-if)# channel-group 1 mode active

*******Subinterface*******
Router(config)# interface Port-channel1*.xx*
Router(config-if)# description LAN
Router(config-if)#encapsulation dot1Q xx
ip address *x.x.x.x y.y.y.y*
ip nat inside
(xx-Port channel number that matches with vlan-id)
(x.x.x.x – p2p ipv4 address)
(y.y.y.y – subnet mask)

*******DHCP*******
Router(config)# ip dhcp excluded-address *x.x.x..1 x.x.x.20*
Router(dhcp-config)# ip dhcp pool *Pool-Name*
Router(dhcp-config)# network *x.x.x.x y.y.y.y*
Router(dhcp-config)# default-router *x.x.x.1*

Router(dhcp-config)# domain-name drukren.bt
Router(dhcp-config)# dns-server 103.197.176.162 8.8.8.8
(x.x.x.1 x.x.x.20 - excluded IP range from 1 to 20)
(Pool-Name - DHCP pool name)
(x.x.x.x - allocated IP block address)
(x.x.x.1 - default IP address)

******* Network Address Translation (NAT) *******
Router(config)# ip nat pool *pool-name x.x.x.x y.y.y.y.y prefix-length 30*
Router(config)# ip nat inside source list *pool-list* pool *pool-name* overload
Router(config)# ip access-list extended *pool-list*
Router(config)# 80 permit ip *a.a.a.a. b.b.b.b* any
(pool-name – NAT pool name)
(pool-list – NAT pool list)
(30 – prefix-length 30 for subnet (/30))
(a.a.a.a – private ipv4 address allocated for the agency)
(b.b.b.b – wildcard mask)

******* Default route configuration *******
Router(config)# ip route 0.0.0.0 0.0.0.0 *x.x.x.x* permanent
(x.x.x.x – core router p2p ipv4 address (next-hop))

Annexure 6(A) - GovNet Core Switch Configuration Template

*******Interface connecting to Agency Router*******
Switch(config)# interface GigabitEthernet0/0/0
Switch(config-if)# description link to agency router
Switch(config-if)# ip address *x.x.x.x y.y.y.y*
(x.x.x.x – p2p ipv4 address)
(y.y.y.y – subnet mask)

*******Interface connecting to Customer Premises Equipment*******
Switch(config)# interface GigabitEthernet0/0/24
Switch(config-if)# description link to CPE
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan *xx*
(x.x.x.x – p2p ipv4 address)
(y.y.y.y – subnet mask)
(xx - vlan_id)

*******DHCP*******
Switch(config)# ip dhcp excluded-address *x.x.x..1 x.x.x.20*
Switch(dhcp-config)# ip dhcp pool *Pool-Name*
Switch(dhcp-config)# network *x.x.x.x y.y.y.y*
Switch(dhcp-config)# default-router *x.x.x.1*
Switch(dhcp-config)# domain-name drukren.bt
(x.x.x.1 x.x.x.20 - excluded IP range from 1 to 20)
(Pool-Name - DHCP pool name)
(x.x.x.x - allocated IP block address)
(x.x.x.1 - default IP address)

*******VLAN*******
Switch(config)# vlan *vlan_id*
Switch(config)# name *vlan_name*
Switch(config)# interface vlan *vlan_id*
Switch(config)# description LAN
Switch(config)# ip address *x.x.x.x y.y.y.y*

*******Default route*******
Switch(config)#*ip route 0.0.0.0 0.0.0.0 x.x.x.x*
(x.x.x.x – agency router p2p ipv4 address (next-hop))

Annexure 6(B) - DrukREN Core Switch Configuration Template

*******Interface Connecting to Agency Router*******
Switch# interface Port-channel1
Switch# description link to agency router
Switch# switchport trunk allowed vlan *xx*
Switch# switchport mode trunk
Switch# channel-group 1 mode active
Switch# interface GigabitEthernet1/0/24
Switch# description link to agency router
Switch# switchport trunk allowed vlan *xx*
Switch# switchport mode trunk
Switch# channel-group 1 mode active
(xx - vlan_id)

*******VLAN*******
Switch(config)# vlan *vlan_id*
Switch(config)# name *vlan_name*

Switch(config-if)# description link to CPE
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan *xx*
(x.x.x.x – p2p ipv4 address)
(y.y.y.y – subnet mask)
(xx - vlan_id)

*******Default Gateway*******
Switch(config)#*ip default-gateway x.x.x.x*
(x.x.x.x – agency router p2p ipv4 address (next-hop))