NETWORK DESIGN GUIDE :

NINJA POSTAL CORPORATION

CONESTOGA
Connect Life and Learning

DESIGNED BY

HARSHUL SHUKLA – 8986048

CONESTOGA COLLEGE

PROF.TOMI OLASIMOJU

Abstract

This project presents the design and implementation of a robust, secure, and scalable network infrastructure for a multinational organization with offices in Tokyo, Vancouver, and Toronto. The network is engineered to address key challenges in inter-office communication, centralized management, and data security, providing a seamless and efficient solution for the company's global operations. The architecture leverages VLAN segmentation, dynamic routing protocols (OSPF/BGP), and centralized Active Directory services to optimize performance, streamline management, and ensure data integrity across geographically dispersed locations.

In addition to ensuring high availability through redundant links and failover mechanisms, the design incorporates comprehensive security measures such as Access Control Lists (ACLs), Role-Based Access Control (RBAC), and end-to-end encryption via TLS and SSH. A disaster recovery plan is integrated to protect critical data, with automated backup systems and remote recovery capabilities. The network design is future-proof, supporting modular expansion and the adoption of emerging technologies like SD-WAN and AI-driven network monitoring. This project successfully aligns with industry standards such as GDPR and HIPAA, ensuring compliance while supporting the organization's growth and operational efficiency.

Table of Contents

Table of Contents 3

Executive Summary 5

Project 6

Scope 6

Objectives 7

Overview of Network Diagram 7

Core Network Components: 7

Network Topology Diagram 9

Configurations 10

CANADA Router_startup-config 10

TOKYO ROUTER_startup-config 12

TOKYO SWITCH 1_startup-config 16

TOKYO SWITCH 2_startup-config 19

TORRONTO Router_startup-config 23

TORRONTO Switch_startup-config 26

VANCOUVER Router_startup-config 29

VANCOUVER Switch_startup-config 32

Design 36

Design Justification 36

Design Overview 38

Guidelines 40

Benefits of Architecture 41

IP Configuration Matrix 42

Security and Compliance Overview 46

Maintaining Network Integrity 47

Data Backup 47
Implementing Firewalls and Access control 47
Security Audits and Continuous Monitoring 47
Compliance with Industry Standards 48
Risk Management and Incident Response 48
Future Proofing and Scalability 49
Technical Landscape 49
Network Design 49
Security 49
Backup Server 50
VLAN 50
Human-Capital Landscape 51
Training 51
Role-Based Access Control 51
Network Optimization 51
References 52
Appendix 53

Executive Summary

This project outlines the design and implementation of a comprehensive, secure, and scalable network infrastructure for a multinational organization with offices located in Tokyo, Vancouver, and Toronto. The organization, operating across geographically dispersed locations, faces the challenge of maintaining efficient, secure communication, centralized management, and support for ongoing growth, all while adhering to international data security regulations such as GDPR and HIPAA. The objective of this project is to address these challenges by designing a robust network that ensures seamless communication, centralized IT management, and business continuity.

The network infrastructure is designed around several core principles: VLAN segmentation, dynamic routing, centralized authentication, and advanced security measures. VLANs segment the network to isolate traffic based on different user roles and departmental requirements, improving security by controlling access and reducing the risk of unauthorized data exposure. Dynamic routing protocols such as OSPF and BGP are implemented to ensure optimized data traffic flow and minimize latency between locations. Additionally, centralized Active Directory integration ensures uniform user authentication across all sites, simplifying management and ensuring consistent access control.

Security is at the forefront of the design. Access Control Lists (ACLs) are used to enforce strict traffic filtering, limiting access to sensitive resources. Role-Based Access Control (RBAC) further ensures that only authorized users can access certain parts of the network based on their role in the organization. All inter-office communication is encrypted using TLS and SSH, safeguarding data in transit from potential threats.

A key component of the design is the disaster recovery and backup strategy. With a centralized backup system located in Tokyo, the project ensures that data can be quickly recovered in the event of a system failure or disaster. The backup system supports both incremental and full backups to maintain data integrity and availability and includes remote access capabilities for emergency recovery. Defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) help minimize downtime and data loss during recovery operations.

The network infrastructure is built with scalability in mind. The modular design allows for easy expansion, enabling the organization to add new offices, departments, or services without disrupting existing operations. The solution also supports emerging technologies such as SD-WAN for enhanced branch connectivity and AI-driven network monitoring tools for proactive issue resolution and network optimization.

In addition to ensuring security and performance, the solution is fully compliant with relevant data protection regulations, including GDPR and HIPAA. By aligning the network design with these legal standards, the project mitigates risks related to data breaches and ensures that the organization's operations are legally compliant across all regions.

Overall, this network infrastructure project provides a future-proof solution that enhances inter-office communication, supports business growth, improves security, and ensures compliance with industry regulations. The design addresses the current and future needs of the organization, positioning it for long-term success.

Project

Scope

This project's primary focus is the design and implementation of a secure, scalable, and efficient network infrastructure that enables smooth communication, centralized IT management, and robust data security for an organization with offices in Tokyo, Vancouver, and Toronto. The scope includes:

1. Designing a multi-site network that connects the three offices while providing optimal performance, security, and reliability.
2. Implementing centralized IT services at the Tokyo headquarters to ensure consistency across all sites.
3. Utilizing VLAN segmentation to improve network security and performance by isolating traffic based on user roles.
4. Configuring dynamic routing protocols to optimize the flow of data and minimize latency across multiple regions.
5. Deploying centralized authentication services to streamline user access management and ensure uniform security policies.
6. Establishing a comprehensive disaster recovery plan with automated backup systems and remote recovery capabilities.
7. Ensuring full compliance with international data security regulations such as GDPR and HIPAA.

Objectives

The key objectives of this network infrastructure project are to:

1. **Enhance Security**: Implement VLANs, firewalls, ACLs, and encryption to safeguard sensitive data and network resources from unauthorized access and cyber threats.
2. **Centralize Management**: Use Active Directory for centralized authentication and policy enforcement, simplifying network management and user access control.
3. **Optimize Performance**: Deploy dynamic routing protocols like OSPF and BGP to ensure efficient use of network resources and minimal latency between offices.
4. **Ensure Business Continuity:** Implement a disaster recovery strategy with centralized backups, automated recovery processes, and clearly defined RTOs and RPOs.
5. **Support Scalability:** Build a modular network architecture that allows for easy integration of new offices, devices, and technologies without major disruptions.
6. **Achieve Regulatory Compliance**: Ensure the network adheres to international standards and regulations like GDPR and HIPAA to protect sensitive data across all regions.

Overview of Network Diagram

The network design for this project incorporates a multi-site architecture to connect the offices in Tokyo, Vancouver, and Toronto. The design emphasizes high availability, security, and scalability by incorporating several key components and strategies.

Core Network Components:

1. **Core Routers:** The central core router in Tokyo serves as the primary point of communication between the Tokyo headquarters and the branch offices in Vancouver and Toronto. It manages the inter-office traffic flow and ensures redundancy through failover mechanisms.

2. **Branch Routers:** Each branch office (Vancouver and Toronto) has its own router, which connects to the core router in Tokyo via secure VPN tunnels or dedicated links. These routers use dynamic routing protocols (OSPF/BGP) to ensure optimal path selection and traffic management between offices.

3. **VLANs and Switches:** LAN segmentation is implemented to isolate traffic based on user roles, ensuring better security and performance. Administrative, general user, and IT services are segmented into separate VLANs, with each VLAN assigned to a dedicated switch. This segregation minimizes congestion and ensures that sensitive data is kept isolated.

4. **Centralized Servers:** A set of centralized servers is hosted in Tokyo to provide critical services such as DNS, Active Directory (AD), file sharing, and web services. These servers are connected to the network through high-performance switches, and each branch office connects to these centralized services for uniform policy enforcement and resource access.

5. **Backup and Disaster Recovery:** A centralized backup system is integrated into the design, located at the Tokyo office. This system performs regular incremental and full backups of critical data and configurations. The backup system supports remote access for disaster recovery, ensuring that data can be recovered quickly in the event of a network failure or natural disaster.

6. **Redundancy and High Availability:** The network design incorporates redundant links between the core and branch routers, as well as between critical servers and switches, to ensure high availability. If a primary connection fails, secondary links automatically take over without causing downtime, ensuring uninterrupted service.

7. **Security Measures:** The design incorporates firewalls, ACLs, and role-based access control (RBAC) to secure the network from external and internal threats. Encryption protocols such as TLS and SSH are used to protect data in transit, while intrusion detection systems (IDS) monitor the network for suspicious activities.

This topology ensures that the network is not only secure and high-performing but also scalable, allowing for easy integration of new offices, devices, or services in the future without disrupting operations.

Network Topology Diagram

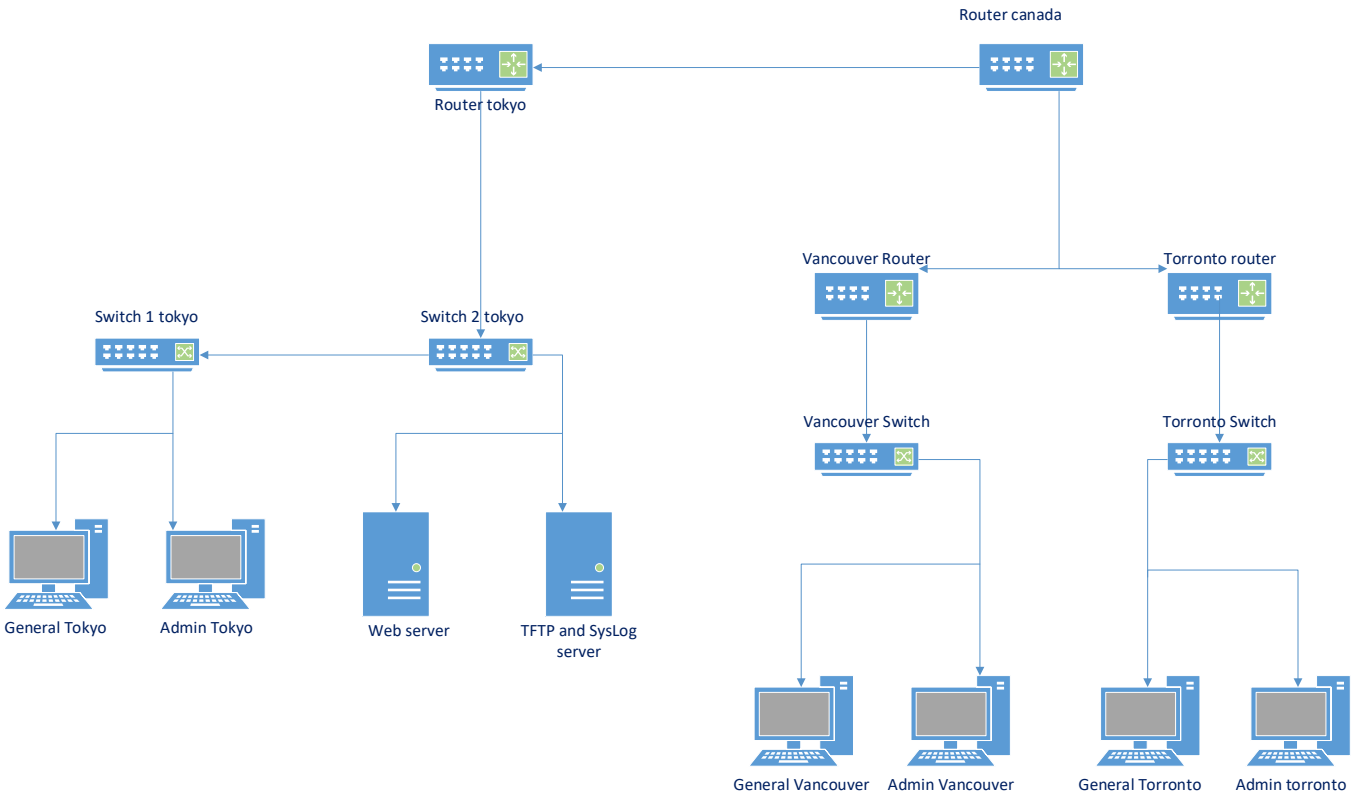

Figure 1 Network Diagram

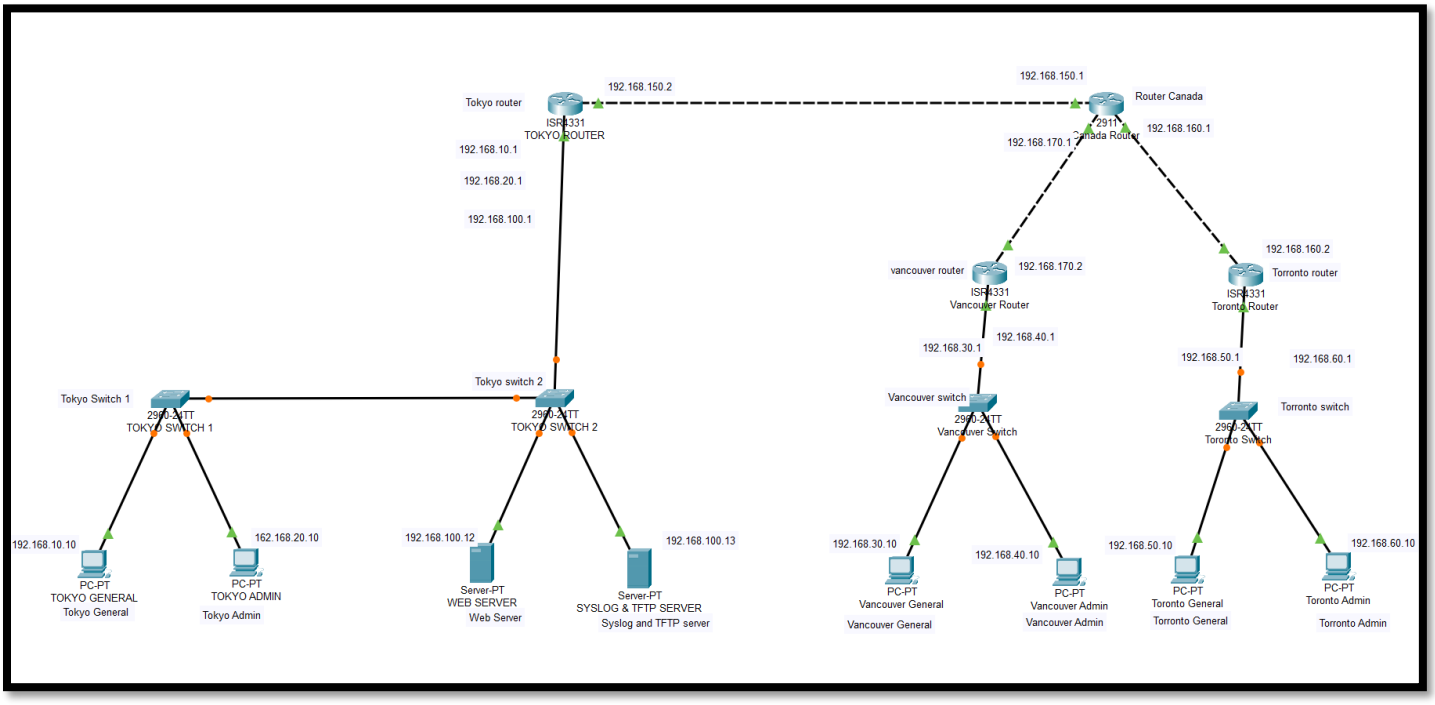

Figure 2 Packet Tracer Diagram

Configurations

CANADA Router_startup-config

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname RCanada
!
enable secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
!
ip cef
no ipv6 cef
!
username Admin privilege 15 secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
username Generaluser privilege 0 secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
username Midleveluser secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
username hshukla6048 privilege 15 secret 5 $1$mERr$2OOvu.7h/I9iaTS3spsWd.
!
license udi pid CISCO2911/K9 sn FTX1524VI1X-
!
ip domain-name D-G3-NINJA
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
 ip address 192.168.150.1 255.255.255.0
 duplex auto
 speed auto
```

```
!
interface GigabitEthernet0/1
 ip address 192.168.170.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 192.168.160.1 255.255.255.0
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 20
 redistribute eigrp 10
 network 192.168.170.0
 network 192.168.160.0
!
router eigrp 10
 redistribute eigrp 20
 network 192.168.150.0
!
router bgp 65004
 bgp log-neighbor-changes
 no synchronization
 neighbor 192.168.150.2 remote-as 65001
 neighbor 192.168.100.1 remote-as 65001
 neighbor 192.168.170.20 remote-as 65002
 neighbor 192.168.170.2 remote-as 65002
```

```
 neighbor 192.168.160.2 remote-as 65003
 network 192.168.170.0
 network 192.168.160.0
!
ip classless
!
ip flow-export version 9
!
banner motd #
UNAUTHORIZED ACCESS RESTRICTED!! THIS IS CANADA ROUTER.#
!
line con 0
 password 7 080F78792241554443
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
!
end
```

TOKYO ROUTER_startup-config

```
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname RTokyo
```

```
!
enable secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
!
no ip cef
no ipv6 cef
!
username Admin privilege 15 secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
username Generaluser privilege 0 secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
username Midleveluser secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
username hshukla6048 privilege 15 secret 5 $1$mERr$2OOvu.7h/I9iaTS3spsWd.
!
ip domain-name D-G3-Ninja
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0/0
 ip address 192.168.150.2 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/0.100
 encapsulation dot1Q 100
 no ip address
!
interface GigabitEthernet0/0/1
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/1.10
 encapsulation dot1Q 10
```

```
 ip address 192.168.10.1 255.255.255.0
 ip access-group 120 in
!
interface GigabitEthernet0/0/1.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
!
interface GigabitEthernet0/0/1.100
 encapsulation dot1Q 100
 ip address 192.168.100.1 255.255.255.0
!
interface GigabitEthernet0/0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 10
 network 192.168.10.0
 network 192.168.150.0
 network 192.168.20.0
 network 192.168.100.0
!
router bgp 65001
 bgp log-neighbor-changes
 no synchronization
 neighbor 192.168.150.1 remote-as 65004
```

```
 neighbor 192.168.170.1 remote-as 65004
 network 192.168.10.0
 network 192.168.20.0
 network 192.168.100.0
!
ip classless
!
ip flow-export version 9
!
!
access-list 120 permit tcp 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255 established
access-list 120 permit icmp 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255 echo-reply
access-list 120 permit tcp 192.168.10.0 0.0.0.255 192.168.40.0 0.0.0.255 established
access-list 120 permit icmp 192.168.10.0 0.0.0.255 192.168.40.0 0.0.0.255 echo-reply
access-list 120 permit tcp 192.168.10.0 0.0.0.255 192.168.60.0 0.0.0.255 established
access-list 120 permit icmp 192.168.10.0 0.0.0.255 192.168.60.0 0.0.0.255 echo-reply
access-list 120 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 120 deny tcp 192.168.50.0 0.0.0.255 eq www host 192.168.100.12
access-list 120 deny tcp 192.168.60.0 0.0.0.255 eq www host 192.168.100.12
access-list 120 permit icmp 192.168.50.0 0.0.0.255 host 192.168.100.12
access-list 120 permit icmp 192.168.60.0 0.0.0.255 host 192.168.100.12
access-list 120 permit ip 192.168.20.0 0.0.0.255 host 192.168.100.12
!
banner motd #
UNAUTHORIZED ACCESS RESTRICTED!! THIS IS TOKYO ROUTER.#
!
logging 192.168.100.13
line con 0
 password 7 080F78792241554443
 login
!
```

```
line aux 0
!
line vty 0 4
 login local
 transport input ssh
!
end
```

TOKYO SWITCH 1_startup-config

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1Tokyo
!
enable secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
!
ip domain-name D-G3-NInja
!
username Admin secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
username Generaluser secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
username Midleveluser secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
username TEST secret 5 $1$mERr$lc2MMSfvTQ6WY4TYsj6TT.
username hshukla6048 secret 5 $1$mERr$2OOvu.7h/I9iaTS3spsWd.
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 10
```

```
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security aging time 2
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security aging time 2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
```

```
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
 switchport trunk allowed vlan 10,20,100
 switchport mode trunk
!
```

```
interface Vlan1
 no ip address
 shutdown
!
banner motd "S1Tokyo : Authorized access only"
logging 192.168.100.13
!
line con 0
 password 7 080F78792241554443
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login
!
end
```

TOKYO SWITCH 2_startup-config

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S2Tokyo
!
enable secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
!
ip domain-name D-G3-Ninja
!
```

```
username Admin secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
username Generaluser secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
username Midleveluser secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
username hshukla6048 secret 5 $1$mERr$2OOvu.7h/I9iaTS3spsWd.
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security aging time 2
!
interface FastEthernet0/2
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security aging time 2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
```

```
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
```

```
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
 switchport trunk allowed vlan 10,20,100
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport trunk allowed vlan 10,20,100
 switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
logging 192.168.100.13
!
line con 0
 password 7 080F78792241554443
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login
!
end
```

TORRONTO Router_startup-config

```
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname RToronto
!
enable secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
!
ip cef
no ipv6 cef
!
username Admin privilege 15 secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
username Generaluser privilege 0 secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
username Midleveluser secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
username hshukla6048 privilege 15 secret 5 $1$mERr$2OOvu.7h/I9iaTS3spsWd.
!
ip domain-name D-G3-Ninja
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/0.50
 encapsulation dot1Q 50
 ip address 192.168.50.1 255.255.255.0
```

```
 ip access-group 120 in
!
interface GigabitEthernet0/0/0.60
 encapsulation dot1Q 60
 ip address 192.168.60.1 255.255.255.0
!
interface GigabitEthernet0/0/1
 ip address 192.168.160.2 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 20
 network 192.168.160.0
 network 192.168.50.0
 network 192.168.60.0
!
router bgp 65003
 bgp log-neighbor-changes
 no synchronization
 neighbor 192.168.160.1 remote-as 65004
 network 192.168.50.0
```

```
 network 192.168.60.0
!
ip default-gateway 192.168.160.10
ip classless
!
ip flow-export version 9
!
access-list 120 permit tcp 192.168.50.0 0.0.0.255 192.168.60.0 0.0.0.255 established
access-list 120 permit icmp 192.168.50.0 0.0.0.255 192.168.60.0 0.0.0.255 echo-reply
access-list 120 permit tcp 192.168.50.0 0.0.0.255 192.168.40.0 0.0.0.255 established
access-list 120 permit icmp 192.168.50.0 0.0.0.255 192.168.40.0 0.0.0.255 echo-reply
access-list 120 permit ip 192.168.50.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 120 permit tcp 192.168.50.0 0.0.0.255 192.168.20.0 0.0.0.255 established
access-list 120 permit icmp 192.168.50.0 0.0.0.255 192.168.20.0 0.0.0.255 echo-reply
access-list 120 permit ip 192.168.50.0 0.0.0.255 192.168.10.0 0.0.0.255
!
banner motd #
UNAUTHORIZED ACCESS RESTRICTED!! THIS IS TORONTO ROUTER.#
!
logging 192.168.100.13
line con 0
 password 7 080F78792241554443
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
!
end
```

TORRONTO Switch_startup-config

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname SToronto
!
enable secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
!
ip domain-name D-G3-Ninja
!
username Admin secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
username Generaluser secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
username Midleveluser secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
username hshukla6048 secret 5 $1$mERr$2OOvu.7h/I9iaTS3spsWd.
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 50
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security aging time 2
!
interface FastEthernet0/2
 switchport access vlan 60
```

```
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security aging time 2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
```

```
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
 switchport trunk allowed vlan 50,60,100
 switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
banner motd #

UNAUTHORIZED ACCESS RESTRICTED!! THIS IS TORONTO SWITCH.#
```

```
logging 192.168.100.13
!
line con 0
 password 7 080F78792241554443
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login
!
end
```

VANCOUVER Router_startup-config

```
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname RVancouver
!
enable secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
!
ip cef
no ipv6 cef
!
username Admin privilege 15 secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
username Generaluser privilege 0 secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
username Midleveluser secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
```

```
username hshukla6048 privilege 15 secret 5 $1$mERr$2OOvu.7h/I9iaTS3spsWd.
!
ip domain-name D-G3-Ninja
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip access-group 120 in
!
interface GigabitEthernet0/0/0.40
 encapsulation dot1Q 40
 ip address 192.168.40.1 255.255.255.0
!
interface GigabitEthernet0/0/1
 ip address 192.168.170.2 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
```

```
interface Vlan1
 no ip address
 shutdown
!
router eigrp 20
 network 192.168.170.0
 network 192.168.30.0
 network 192.168.40.0
!
router bgp 65002
 bgp log-neighbor-changes
 no synchronization
 neighbor 192.168.170.1 remote-as 65004
 network 192.168.30.0
 network 192.168.40.0
!
ip default-gateway 192.168.170.10
ip classless
!
ip flow-export version 9
!
!
access-list 120 permit tcp 192.168.30.0 0.0.0.255 192.168.40.0 0.0.0.255 established
access-list 120 permit icmp 192.168.30.0 0.0.0.255 192.168.40.0 0.0.0.255 echo-reply
access-list 120 permit tcp 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255 established
access-list 120 permit icmp 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255 echo-reply
access-list 120 permit ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 120 permit tcp 192.168.30.0 0.0.0.255 192.168.60.0 0.0.0.255 established
access-list 120 permit icmp 192.168.30.0 0.0.0.255 192.168.60.0 0.0.0.255 echo-reply
access-list 120 permit ip 192.168.30.0 0.0.0.255 192.168.50.0 0.0.0.255
!
```

```
banner motd #
UNAUTHORIZED ACCESS RESTRICTED!! THIS IS VANCOUVER ROUTER.#
!
logging 192.168.100.13
line con 0
 password 7 080F78792241554443
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
!
end
```

VANCOUVER Switch_startup-config

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname SVancouver
!
enable secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
!
ip domain-name D-G3-Ninja
!
username Admin secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
username Generaluser secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
```

```
username Midleveluser secret 5 $1$mERr$YwrQWPAs/7SoRRJPR9dmD.
username hshukla6048 secret 5 $1$mERr$2OOvu.7h/I9iaTS3spsWd.
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 30
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security aging time 2
!
interface FastEthernet0/2
 switchport access vlan 40
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security aging time 2
!
interface FastEthernet0/3
 switchport access vlan 30
 switchport mode access
 shutdown
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
```

interface FastEthernet0/7

!

interface FastEthernet0/8

!

interface FastEthernet0/9

!

interface FastEthernet0/10

!

interface FastEthernet0/11

!

interface FastEthernet0/12

!

interface FastEthernet0/13

!

interface FastEthernet0/14

!

interface FastEthernet0/15

!

interface FastEthernet0/16

!

interface FastEthernet0/17

!

interface FastEthernet0/18

!

interface FastEthernet0/19

!

interface FastEthernet0/20

!

interface FastEthernet0/21

!

interface FastEthernet0/22

```
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
 switchport trunk allowed vlan 30,40,100
 switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
banner motd #
UNAUTHORIZED ACCESS RESTRICTED!! THIS IS VANCOUVER SWITCH.#
logging 192.168.100.13
!
line con 0
 password 7 080F78792241554443
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login
!
end
```

Design

Design Justification

The design of the network infrastructure for this multinational organization is driven by key principles aimed at optimizing performance, enhancing security, ensuring scalability, and enabling centralized management. The decisions made in each aspect of the design are justified based on the specific needs of the organization and its operational goals, ensuring long-term reliability and adaptability.

1. **Security by Design:**

VLAN Segmentation: One of the most crucial design decisions was the use of VLANs (Virtual Local Area Networks) to segment network traffic based on user roles and functional areas. This isolation reduces the risk of unauthorized access by creating distinct communication zones within the network. For example, administrative VLANs are isolated from general user traffic, ensuring that sensitive administrative data is protected from non-privileged users. Similarly, IT services such as servers and network management tools are placed in a dedicated VLAN to ensure security and minimize exposure.

Access Control Lists (ACLs) and Role-Based Access Control (RBAC): These security measures were implemented to restrict access to network resources based on roles and defined policies. ACLs filter traffic by IP addresses and ports, ensuring that only authorized devices or users can communicate with specific resources. RBAC further strengthens access control by assigning permissions based on the user's role within the organization, ensuring that only individuals with appropriate privileges can access sensitive data or services.

2. **Scalability:**

Modular Network Architecture: The network is designed with scalability in mind, ensuring that it can grow seamlessly as the organization expands. The use of modular components such as routers, switches, and VLANs enables the easy addition of new offices, departments, or devices without disrupting existing operations. By using dynamic routing protocols such as OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol), the network can adapt to new geographical locations and handle an increasing volume of data traffic efficiently.

Software-Defined Networking (SDN): As part of future-proofing the infrastructure, the design supports the integration of SD-WAN (Software-Defined Wide Area Network) in the future, allowing the organization to take advantage of lower-cost broadband connections while maintaining optimal network performance and security.

3. **Efficiency and Performance:**

Dynamic Routing Protocols (OSPF/BGP): These protocols ensure that network traffic is routed dynamically and efficiently between the three offices. OSPF, an interior gateway protocol, is used within the local networks of each office, while BGP is deployed for inter-office communication, providing optimal paths for data flow and minimizing latency. The dynamic nature of these protocols allows the network to automatically adjust to any changes in topology, such as link failures or new office additions, ensuring continued performance.

High-Availability Configuration: To prevent service disruptions, redundant links and failover mechanisms are integrated into the design. This ensures that if one path fails, data can be rerouted through alternative routes without affecting business operations. Redundancy is crucial in maintaining uptime and reliability, especially for mission-critical services like web hosting, file sharing, and centralized authentication.

4. **Centralized Management:**

Active Directory (AD) Integration: Centralized user authentication and access control are provided through Active Directory. By hosting Active Directory servers in Tokyo, the organization ensures that all users, regardless of their physical location, adhere to the same security policies and have consistent access to network resources. This centralization simplifies IT management by providing a single point for managing user credentials, group policies, and permissions.

Centralized Backup System: The centralized backup strategy, also hosted in Tokyo, provides consistency in data protection across all locations. Regular backups ensure that critical data is always available for recovery, while remote access capabilities allow for recovery in the event of a disaster.

5. **Compliance with Industry Standards:**

The network infrastructure is designed to comply with relevant international data security regulations, including GDPR (General Data Protection Regulation) and HIPAA (Health Insurance Portability and Accountability Act). GDPR compliance ensures that personal data is handled and stored in accordance with European privacy laws, while HIPAA compliance addresses the protection of healthcare-related data. The use of encryption, secure authentication methods, and access control mechanisms guarantees that the network adheres to these regulations, protecting both the organization and its customers from potential data breaches and legal penalties.

Design Overview

The network infrastructure is designed to support the organization's global operations, ensuring seamless communication between offices, secure data management, and the ability to scale as needed. The key components of the design are outlined below:

1. **Core Network:**

Core Router in Tokyo: The core router in Tokyo serves as the central hub for communication between the three offices. It is responsible for managing traffic between the local area networks (LANs) in Tokyo, Vancouver, and Toronto, ensuring optimal routing and connectivity.

Branch Routers in Vancouver and Toronto: Each branch office has its own router that connects to the Tokyo core router, providing redundancy and ensuring that the network can withstand the failure of any single link.

2. **VLAN Segmentation**:

Admin VLAN: A dedicated VLAN for administrative users, ensuring that only authorized personnel have access to sensitive administrative resources.

General User VLAN: A VLAN for general employees, isolating their traffic from sensitive organizational data and improving network efficiency by preventing unnecessary congestion.

IT Services VLAN: A VLAN dedicated to infrastructure services like file sharing, web hosting, and network management tools, ensuring that these critical resources are isolated from other user traffic and remain highly available.

3. **Redundancy and High Availability:**

Redundant Links: The network includes redundant links between the core router and branch offices, as well as between critical servers and network devices. This ensures that if one link or device fails, the network will automatically reroute traffic through another available path.

Load Balancing: To improve performance, load balancing is implemented between network paths, ensuring that no single route becomes a bottleneck and that resources are optimally utilized.

4. **Security Measures:**

Firewalls: Positioned at the network boundaries, firewalls control incoming and outgoing traffic, ensuring that only authorized traffic is allowed into and out of the network.

Encryption: All inter-office communication is encrypted using TLS and SSH, ensuring that sensitive data is protected from eavesdropping and tampering.

Intrusion Detection Systems (IDS): IDS systems are used to monitor network traffic for suspicious activity, alerting administrators to potential security threats.

5. **Disaster Recovery and Backup:**

Centralized Backup: The backup system in Tokyo ensures that critical data and configurations are regularly backed up and available for recovery. The system supports both full and incremental backups to minimize storage requirements and recovery times.

Disaster Recovery Plan: The disaster recovery plan includes defined RTOs and RPOs, ensuring that the organization can recover data quickly and resume operations in the event of a network or system failure.

6. **Scalability and Future-Proofing:**

Modular Design: The network is built with a modular design, allowing for easy expansion. New offices, devices, or services can be added without disrupting existing operations.

Support for Emerging Technologies: The design includes provisions for integrating new technologies like SD-WAN and AI-driven network monitoring as the organization grows, ensuring that the network can evolve with the business and technological advancements.

Guidelines

The network design incorporates two autonomous systems: one for the Tokyo office in Japan and another for the Canadian offices located in Toronto and Vancouver. This segmentation ensures efficient traffic routing and manageable data flow across the network. By leveraging dynamic routing protocols such as OSPF and BGP, the design ensures optimal traffic management between the two regions, reducing latency and improving overall network performance.

A centralized Web Server is hosted in the Tokyo office, accessible only by authorized users through stringent access control policies, ensuring both security and data integrity. To further enhance security, Port Security is implemented across the network to limit access to authorized devices and prevent unauthorized connections, safeguarding the network from potential security breaches.

In each of the three offices (Tokyo, Toronto, and Vancouver), VLANs are carefully segregated for administrative users and general users. This VLAN-based architecture ensures that sensitive administrative traffic is isolated from regular user traffic, improving security and preventing unauthorized access to critical resources. This segmentation not only enhances security but also improves network performance by reducing unnecessary traffic congestion between different user groups.

The Tokyo office is also home to centralized services, which include essential resources such as central backup systems and TFTP (Trivial File Transfer Protocol) services. These services are made available to all offices, ensuring data reliability and availability across the organization. By centralizing services such as backups, TFTP, and web hosting in Tokyo, the network guarantees efficient data management, streamlined accessibility, and easier administration across all locations. This centralization enhances data consistency, ensures rapid recovery during data loss, and simplifies IT management tasks by consolidating key services in a single location.

Overall, this approach promotes better network security, simplifies administrative overhead, and ensures that all users and devices across the three offices are able to access the necessary resources while maintaining the integrity and security of the entire network infrastructure.

Benefits of Architecture

The proposed network architecture offers significant benefits across security, performance, scalability, and management. By addressing key challenges, the design enhances the overall efficiency of the organization while ensuring it is future-proof and compliant with industry standards.

1. Enhanced Security

VLAN Segmentation isolates traffic based on user roles, reducing the risk of unauthorized access and ensuring sensitive data is protected.

Port Security and Access Control limit network access to authorized devices and users, enhancing security at the network's entry points.

Encryption (TLS/SSH) ensures secure communication between offices, safeguarding data during transmission.

2. Improved Network Performance

Dynamic Routing (OSPF/BGP) optimizes traffic flow between offices, minimizing latency and maximizing bandwidth utilization.

VLAN Separation reduces congestion by isolating traffic based on function, ensuring smoother communication and better resource management.

3. Scalability and Flexibility

Modular Network Design allows for easy expansion as the organization grows. New offices, services, or devices can be added without disrupting operations.

Support for Emerging Technologies like SD-WAN and AI-driven network monitoring tools ensures the network can evolve with the organization.

4. Centralized Management and Simplified Administration

Active Directory Integration simplifies user authentication and policy enforcement, ensuring consistent access across all locations.

Centralized Services (DNS, backups, web hosting) in Tokyo reduce redundancy and streamline network management, improving efficiency.

5. High Availability and Disaster Recovery

Redundant Links and failover mechanisms ensure high availability, automatically rerouting traffic in case of failure to minimize downtime.

Centralized Backup System provides automated backups, ensuring rapid data recovery in the event of network failure or disaster.

6. Compliance and Data Protection

The network design ensures GDPR and HIPAA compliance by implementing strong data protection measures, including encryption, secure communication, and access control.

IP Configuration Matrix

Device	Location	IP Address	Subnet Mask	VLAN ID	Role
Router1	Tokyo	192.168.1.1	255.255.255.0	N/A	Core Router
Switch1	Tokyo	192.168.1.2	255.255.255.0	N/A	Core Switch
Server1 (Web)	Tokyo	192.168.10.10	255.255.255.0	10	Web Server
PC1 (Admin)	Tokyo	192.168.20.10	255.255.255.0	20	Admin PC
Router2	Vancouver	192.168.2.1	255.255.255.0	N/A	Core Router
Switch2	Vancouver	192.168.2.2	255.255.255.0	N/A	Core Switch
PC2 (General)	Vancouver	192.168.30.10	255.255.255.0	30	General PC
Router3	Toronto	192.168.3.1	255.255.255.0	N/A	Core Router
Switch3	Toronto	192.168.3.2	255.255.255.0	N/A	Core Switch
PC3 (Admin)	Toronto	192.168.40.10	255.255.255.0	40	Admin PC

Router1
Device Name: TOKYO ROUTER
Location: Tokyo

Port	IP Address	Subnet Mask
GigabitEthernet0/0/0	192.168.150.2	255.255.255.0
GigabitEthernet0/0/1.10	192.168.10.1	255.255.255.0
GigabitEthernet0/0/1.20	192.168.20.1	255.255.255.0
GigabitEthernet0/0/1.100	192.168.100.1	255.255.255.0

Switch 1
Device Name: TOKYO SWITCH 1
Location: Tokyo

Port	VLAN
FasthEthernet0/1	10
FastEthernet0/2	20

Switch 2
Device Name: TOKYO SWITCH 2
Location: Tokyo

Port	VLAN
FastEthernet0/1	100
FastEthernet0/2	100

PC 1
Device Name: TOKYO ADMIN
Location: Tokyo

Port	IP Address	Subnet Mask	Default Gateway
FastEthernet0	192.168.20.10	255.255.255.0	192.168.20.1

PC 2
Device Name: TOKYO GENERAL
Location: Tokyo

Port	IP Address	Subnet Mask	Default Gateway
FastEthernet0	192.168.10.10	255.255.255.0	192.168.10.1

Server 1
Device Name: WEB SERVER
Location: Tokyo

Port	IP Address	Subnet Mask	Default Gateway
FastEthernet0	192.168.100.12	255.255.255.0	192.168.100.1

Server 2
Device Name: SYSLOG & TFTP SERVER
Location: Tokyo

Port	IP Address	Subnet Mask	Default Gateway
FastEthernet0	192.168.100.13	255.255.255.0	192.168.100.1

Router 3
Device Name: Canada Router
Location: Canada

Port	IP Address	Subnet Mask
GigabitEthernet0/0	192.168.150.1	255.255.255.0
GigabitEthernet0/1	192.168.170.1	255.255.255.0
GigabitEthernet0/2	192.168.160.1	255.255.255.0

Router 3
Device Name: Vancouver Router
Location: Vancouver

Port	IP Address	Subnet Mask	Default Gateway
GigabitEthernet0/0/0.30	192.168.30.1	255.255.255.0	192.168.170.10
GigabitEthernet0/0/0.40	192.168.40.1	255.255.255.0	192.168.170.10
GigabitEthernet0/0/1	192.168.170.2	255.255.255.0	192.168.170.10

Router 4
Device Name: Toronto Router
Location: Toronto

Port	IP Address	Subnet Mask	Default Gateway
GigabitEthernet0/0/0.50	192.168.50.1	255.255.255.0	192.168.160.10
GigabitEthernet0/0/0.60	192.168.60.1	255.255.255.0	192.168.160.10
GigabitEthernet0/0/1	192.168.160.2	255.255.255.0	192.168.160.10

Switch 3
Device Name: Vancouver Switch
Location: Vancouver

Port	VLAN
FastEthernet0/1	30
FastEthernet0/2	40
FastEthernet0/3	30

Switch 4
Device Name: Toronto Switch
Location: Toronto

Port	VLAN
FastEthernet0/1	50
FastEthernet0/2	60

PC 3
Device Name: Vancouver Admin
Location: Vancouver

Port	IP Address	Subnet Mask	Default Gateway
FastEthernet0	192.168.40.10	255.255.255.0	192.168.40.1

PC 4
Device Name: Vancouver General
Location: Vancouver

Port	IP Address	Subnet Mask	Default Gateway
FastEthernet0	192.168.30.10	255.255.255.0	192.168.30.1

PC 5
Device Name: Toronto Admin
Location: Toronto

Port	IP Address	Subnet Mask	Default Gateway
FastEthernet0	192.168.60.10	255.255.255.0	192.168.60.1

PC 6
Device Name: Toronto General
Location: Toronto

Port	IP Address	Subnet Mask	Default Gateway
FastEthernet0	192.168.50.10	255.255.255.0	192.168.50.1

Security and Compliance Overview

The design of Ninjapostal's network prioritizes robust security measures to safeguard data across our offices in Tokyo, Toronto, and Vancouver. We have implemented multiple layers of defense to prevent unauthorized access, including the application of Access Control Lists (ACLs) to regulate traffic flow between VLANs. Additionally, Role-Based Access Control (RBAC) ensures that only authorized personnel can access sensitive devices and systems, while admin users are granted exclusive access to critical network components.

Our network security is further bolstered by continuous monitoring through syslog, which tracks and logs all security incidents and activities. This allows for real-time detection and swift response to potential threats. In Tokyo, a centralized backup system is maintained via a TFTP server, providing secure storage and ensuring efficient, reliable restoration of network configurations in case of an emergency.

Our network is fully compliant with industry-leading regulations such as HIPAA (Rights, 2022) and GDPR (PIPEDA vs. GDPR | A Comprehensive Guide to Data Privacy Laws in Canada and the EU, 2024). These frameworks are critical to protecting sensitive data and ensuring our operations remain legally compliant, mitigating the risks of non-compliance penalties.

Regular data backups are performed with stringent security protocols in place, including firewalls and routine security audits, to ensure both the integrity and confidentiality of our data. These efforts collectively prevent unauthorized access and safeguard against potential data breaches.

By prioritizing comprehensive security measures and compliance with global data privacy laws, we ensure the protection of our business operations and customer information. This commitment not only enhances data security but also bolsters our company's reputation, fosters customer trust, and safeguards against legal penalties—ultimately supporting the long-term success and operational continuity of our business.

Maintaining Network Integrity

Data Backup

To ensure the security, availability, and integrity of all critical data, our centralized backup server located in Tokyo, Japan, serves as a cornerstone of our data protection strategy. This backup system is regularly updated through daily automated backups, which not only safeguard against potential data loss but also ensure fast recovery in case of system failure. Our backup process leverages industry-best practices, including encryption of sensitive data both at rest and in transit, ensuring that backup copies remain secure and confidential. Additionally, versioning and off-site storage further enhance our disaster recovery capabilities, enabling quick restoration of critical network configurations and preventing data corruption from impacting business continuity.

Implementing Firewalls and Access control

We have deployed multiple layers of defense to control access to our network. Access Control Lists (ACLs) are carefully configured to ensure that only authorized users can access sensitive data. Role-Based Access Control (RBAC) is implemented across the organization, ensuring that users are granted access to only the resources necessary for their job functions. Admin users enjoy full access, while other users are restricted based on their role and permissions. In addition to ACLs, we implement firewall rules at various network entry points to further segment traffic and block unauthorized attempts to reach critical systems or data. These firewalls not only enforce the principle of least privilege but also provide a first line of defense against potential threats, protecting customer information and ensuring network integrity.

Security Audits and Continuous Monitoring

Our commitment to network security is underscored by our regular security audits, which are conducted on a quarterly basis. These audits involve a comprehensive review of our infrastructure, including penetration testing, vulnerability assessments, and compliance checks against industry standards such as ISO/IEC 27001, HIPAA, and GDPR. By identifying potential risks and gaps in our defenses, we take proactive steps to remediate vulnerabilities before they can be exploited. Furthermore, our audits assess the effectiveness of existing security controls, ensuring that they align with evolving threats and industry best practices.

In addition to scheduled audits, we employ continuous network monitoring to detect any unusual or suspicious activity in real-time. This monitoring system integrates with our incident response plan, enabling rapid identification and containment of security breaches. Alerts are immediately generated for abnormal traffic patterns or unauthorized access attempts, ensuring that our security team can respond swiftly to mitigate potential damage.

Compliance with Industry Standards

We are committed to maintaining full compliance with relevant industry regulations, including GDPR, HIPAA, and ISO 27001, ensuring that all data handling and processing activities are conducted in accordance with legal requirements. Compliance is not just about meeting regulatory standards but also about building a culture of trust with our clients. Through continuous training and adherence to security protocols, we ensure that our employees and partners remain vigilant and well-informed about their roles in maintaining network security.

Risk Management and Incident Response

Our network security strategy also includes a comprehensive risk management framework. We regularly assess both internal and external risks to identify potential threats that could affect the integrity of our network. This proactive approach allows us to develop and implement mitigation strategies to address emerging risks. In the event of a security incident, our incident response team follows a well-defined protocol to quickly contain, investigate, and remediate the issue. Post-incident reviews are conducted to assess the effectiveness of the response and to update policies or defenses as needed to prevent recurrence.

Through a combination of data backups, firewall implementations, security audits, and continuous monitoring, we ensure the ongoing integrity and security of our network. These efforts not only protect sensitive data but also foster trust with our customers, stakeholders, and regulatory bodies, ensuring that we remain resilient against threats while maintaining operational continuity.

Future Proofing and Scalability

Our network architecture is designed with a scalable and future-proof approach, ensuring that it can evolve in parallel with the organization's growth and technological advancements. Whether adding a new server, device, or expanding to new office locations, the system is built to seamlessly accommodate these changes. By implementing dynamic routing, VLANs, and Role-Based Access Control (RBAC), the network can efficiently handle increased demand, expanding user bases, and new services, all while ensuring smooth operations and uninterrupted service delivery.

The flexibility of this design allows for easy scaling and integration of additional resources without the need for major overhauls, making the organization well-prepared for future growth. Additionally, our centralized TFTP and backup system in Tokyo provides streamlined data management, ensuring that backups are regularly updated and easily recoverable in the event of network failures or disasters. This setup allows for quick recovery and reduces downtime, simplifying the administrative workload and ensuring business continuity even during unexpected issues.

Technical Landscape

Network Design

The network design is optimized for both scalability and reliability. By leveraging dynamic routing and VLANs, the network can grow with the organization’s evolving needs, enabling seamless integration of new offices, user groups, and services. This design minimizes operational disruptions, ensuring smooth network expansion without performance degradation. It also provides a robust foundation for future upgrades, as the network can easily accommodate higher traffic volumes and additional devices. The ability to scale quickly and efficiently is a core strength of this architecture, making it ideal for businesses with expanding needs.

Security

Port security is implemented to prevent unauthorized physical access to network devices. This security feature is designed to block attempts by unauthorized users to connect to the network, thus reducing the risk of data theft or malicious activity. By limiting physical access to devices, we mitigate potential security breaches and protect the integrity of the network, ensuring that only legitimate, authorized devices can interact with critical infrastructure.

Backup Server

A centralized backup system in Tokyo ensures that all critical data is regularly backed up and can be easily restored in the event of a disaster or network failure. The backup infrastructure is designed to be resilient, supporting multiple recovery methods to ensure business continuity during emergencies, such as natural disasters like storms or earthquakes. Additionally, remote access capabilities enable administrators to manage and restore backups from any location, further enhancing the system's flexibility and reliability.

VLAN

Virtual Local Area Networks (VLANs) are a fundamental component of the network design, offering a highly efficient way to manage network traffic, enhance security, and improve performance. VLANs allow the network to be segmented based on user roles and functions, ensuring that sensitive data is isolated and protected while optimizing traffic flow. Each VLAN is configured with its own unique IP address range, simplifying network management and troubleshooting. This segmentation makes it easy to add new user groups, offices, or services without disrupting the existing network, ensuring seamless expansion and minimal impact on operations. The use of VLANs also improves the overall security posture by reducing the attack surface and controlling access to critical resources based on user needs.

Human-Capital Landscape

Training

Ongoing training sessions for our IT staff ensure they remain up-to-date with the latest industry best practices and management techniques. These training programs cover a broad range of topics, including network configurations, protocols, security best practices, troubleshooting, and compliance with industry standards. By investing in regular training, we ensure that our team is capable of efficiently managing the network and addressing any challenges that arise, maintaining a secure and high-performance network environment.

Role-Based Access Control

We have implemented Role-Based Access Control (RBAC) to ensure that only authorized personnel can access sensitive data. Three distinct roles have been defined, each with its own permissions and restrictions, based on the user's responsibilities. This layered approach ensures that data integrity and security are maintained by granting access only to those who absolutely need it, minimizing the risk of unauthorized access or data breaches. This control mechanism ensures that access to critical systems and data is managed efficiently and securely.

Network Optimization

We are committed to ongoing network optimization to ensure the system performs efficiently and can scale with the company's growth. Regular performance checks, network analysis, and adjustments are made to maintain optimal performance and reliability. These efforts ensure that the network can handle increasing workloads, support growing user demands, and sustain high levels of user satisfaction. By proactively managing the network's performance, we are able to address potential bottlenecks, enhance reliability, and ensure seamless operation even as the organization evolves.

References

Auth. (n.d.). *Role-Based access control*. Auth0 Docs. https://auth0.com/docs/manage-users/access-control/rbac

GeeksforGeeks. (2023, January 1). *Switch concepts and configuration*. GeeksforGeeks. https://www.geeksforgeeks.org/switch-concepts-and-configuration/

Network design for effective security and performance simplified. (n.d.). https://www.garlandtechnology.com/blog/network-design-for-effective-security-and-performance-simplified

PIPEDA vs GDPR | A Comprehensive Guide to Data Privacy Laws in Canada and the EU. (2024, July 30). https://secureprivacy.ai/. https://secureprivacy.ai/blog/pipeda-vs-gdpr-comprehensive-guide#:~:text=Ensuring%20the%20security%20of%20personal,Data%20Protection%20Regulation%20(GDPR).

Rights, O. F. C. (2022, October 19). *Summary of the HIPAA Privacy Rule*. HHS.gov. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

What is BGP? - BGP Routing Explained - AWS. (n.d.). Amazon Web Services, Inc. https://aws.amazon.com/what-is/border-gateway-protocol/#:~:text=Border%20Gateway%20Protocol%20(BGP)%20is,%2C%20devices%2C%20and%20communication%20technologies.

What is network scalability? How to optimize for growth | Nile. (2024, August 6). Nile. https://nilesecure.com/network-design/network-scalability#:~:text=Network%20scalability%20refers%20to%20the,performance%20remains%20stable%20and%20reliable.

Appendix

Full Forms:

ACL - Access Control List

AS - Autonomous System

BYOD - Bring Your Own Device

CCTV - Closed-Circuit Television

C-level - Chief Level (e.g., CEO, CFO, CIO)

GDPR - General Data Protection Regulation

HIPAA - Health Insurance Portability and Accountability Act

IP - Internet Protocol

RBAC - Role-Based Access Control

SSH - Secure Shell

TFTP - Trivial File Transfer Protocol

TLS - Transport Layer Security

VLAN - Virtual Local Area Network

Tools Used:

Microsoft Word, Microsoft Visio, Microsoft Excel, Cisco Packet Tracer