IUBAT

International University of Business Agriculture & Technology

Course Title: Data Communication and Computer Networking

Course Code: CSC 465

Final Assignment

Topic: Report for Inspire IT Solutions with Multiple Offices in Bangladesh

Submitted By:

Name: Aononto Jahan Junnurain
ID: 21103030
Program: BCSE
Section: I

Submitted To:

Mahedi Hasan
Lecturer,
Department of CSE

Submission Date: 25-09-2025

Table of Contents

Report for Inspire IT Solutions with Multiple Offices in Bangladesh

1. Executive Summary

This report presents the comprehensive network design for Inspire IT Solutions, a fast-growing IT company with its headquarters in Dhaka and a branch office in Chattogram, along with a team of remote developers across Bangladesh. The company is looking to deploy a scalable, high-performance, and secure network infrastructure that not only connects the two offices but also facilitates seamless access for remote employees. The goal is to ensure robust connectivity and operational continuity while supporting the company's future growth.

The network design includes a set of essential components that ensure secure, efficient, and reliable communication across multiple sites:

a. VLANs: To logically segment network traffic by department (e.g., administration, development, testing) for improved security and efficient use of bandwidth.

b. Secure Inter-office Connectivity: A site-to-site VPN is implemented between the Dhaka and Chattogram offices, enabling encrypted communication and ensuring data privacy across public networks.

c. Wireless Networking: The design incorporates wireless access points to provide reliable Wi-Fi coverage within office spaces, ensuring employees have flexibility in their workspaces.

d. Remote Developer VPN Access: A secure VPN solution is designed to allow remote developers to access internal resources, ensuring that the company's work-from-home policies and flexible work arrangements do not compromise security.

Key decisions in protocol selection and network architecture have been made based on performance requirements, security considerations, and the company's growth potential. Protocols like TCP, UDP, IPsec, and OSPF are strategically chosen to balance reliability, speed, and security, allowing the company to maintain a high level of performance while protecting sensitive data. Additionally, the network architecture is designed to ensure scalability, enabling the company to easily accommodate a 20% increase in devices and users over the next two years.

The design emphasizes high availability and reliability to support mission-critical services like video conferencing, file sharing, and collaborative development, ensuring that Inspire IT Solutions remains competitive in the ever-evolving IT industry.

2. Problem Analysis and Performance Factors

Inspire IT Solutions operates from two primary locations—Dhaka (Headquarters) and Chattogram with a workforce that includes remote developers located across Bangladesh. The company is rapidly growing and requires a high-performance, scalable, and secure network to ensure seamless operations between its headquarters, branch office, and remote workers. The network must support the company's increasing demand for bandwidth-intensive applications, secure remote access, and high availability to ensure smooth business operations.

Key Technical Requirements

a. High-speed Internet Connectivity: The network must support high-speed internet connections in both offices and for remote developers, ensuring efficient access to cloud resources, web applications, and the company's internal resources.

b. VLAN Configuration: The company needs VLANs to logically separate traffic across different departments (e.g., Administration, Development, Testing, Sales, and Customer Support). This will improve security, reduce broadcast traffic, and ensure efficient network performance.

c. Secure Communication: The Dhaka and Chattogram offices must have secure communication channels for accessing shared resources, using a site-to-site VPN to ensure data privacy and integrity. Remote developers must also have secure access to the internal network via a VPN solution that provides encryption and secure user authentication.

d. Wireless Connectivity: Both offices require Wi-Fi for mobility within office spaces. Additionally, the wireless network should be optimized to handle both employee devices and guest users without compromising network performance or security.

e. Scalability: With a projected 20% increase in devices and users over the next two years, the network must be designed to scale without major changes. This includes having sufficient bandwidth, IP address allocation, and resources to support future growth.

Performance-Impacting Parameters

a. Bandwidth: The network must offer high throughput to accommodate the increasing volume of data traffic, especially for applications such as video conferencing, file sharing, and real-time collaboration between teams. Departments like Development and Testing, which require large data transfers and access to cloud-based applications, will particularly benefit from sufficient bandwidth.

b. Latency: Low latency is critical for real-time communication, including video conferencing, VoIP, and remote development tools used by employees in both offices and remote locations. Delays in data transmission could result in poor user experiences, reduced productivity, and communication breakdowns. The design should minimize network delays, particularly between the two offices and for remote users accessing internal applications.

c. Reliability: To ensure that business operations are not interrupted, redundancy and failover mechanisms should be implemented in key areas of the network, including inter-office connectivity and remote access. For example, redundant VPN tunnels or backup internet links should be considered to guarantee that critical communication between the Dhaka and Chattogram offices remains uninterrupted.

d. Availability: The network must be available 24/7 to support remote developers who require constant access to company resources, regardless of time zones. The design should prioritize high availability for mission-critical services like VoIP, video conferencing, and collaboration tools. This includes ensuring that the network is resilient to outages and that appropriate measures are taken to monitor and quickly restore connectivity if a failure occurs.

Mapping Business Needs with Technical Requirements

a. Remote Work: With remote developers scattered across Bangladesh, there is a critical need for secure remote access to ensure that all employees can collaborate effectively and access the company's resources securely. The VPN solution will address this need, providing encrypted communication channels for remote workers.

b. Scalability: As the company expects growth in both office and remote users, the network must be designed with future scalability in mind. This includes ensuring that the network can easily support an additional 20% growth in devices and users without requiring a complete overhaul of the infrastructure.

c. Secure Access: Security is paramount, especially for remote workers and communication between offices. The use of site-to-site VPNs, firewall rules, and secure authentication mechanisms ensures that the network will remain protected from unauthorized access, while allowing employees to securely access the data and resources they need to perform their tasks.

3. Theoretical Justification of Communication Methods

In this section, we describe and justify the communication protocols, access methods, and addressing models chosen for the network design of Inspire IT Solutions. These decisions are based on the company's needs for reliability, scalability, security, and performance.

Protocols

1. Transmission Control Protocol (TCP)
   TCP is chosen for most communication types in the network due to its reliability and connection-oriented nature. TCP ensures that data is delivered without errors and in the correct order, making it ideal for applications where data integrity is critical. For example, TCP is used for file transfers, web access, and application hosting. Its mechanisms, such as error checking and retransmission of lost packets, guarantee that information is delivered successfully even in cases of network congestion or error.

   - Justification: TCP's flow control and congestion control mechanisms ensure that the network performs optimally even during high traffic periods. This is especially important for departments like Development and Testing, where large files need to be transferred and data integrity must be maintained.

   - Data Communication Principles: TCP ensures reliable data delivery using window-based flow control and sequence numbering, which ensures the proper order of packets. The protocol operates within the transport layer of the OSI model and requires handshaking between the sender and receiver.

2. User Datagram Protocol (UDP)
   UDP is used for real-time services like VoIP (Voice over IP) and video conferencing, where low latency is more important than reliability. Unlike TCP, UDP does not guarantee data delivery, which minimizes overhead and allows for faster transmission of data packets. This is crucial for services that require immediate feedback, such as video calls and online meetings.

   - Justification: UDP is ideal for applications where small amounts of lost data can be tolerated, and where reducing the delay is a higher priority than ensuring perfect delivery. For example, during video conferences, a slight packet loss does not significantly degrade the quality of the call but reducing latency is essential for real-time communication.

   - Data Communication Principles: UDP operates at the transport layer of the OSI model and uses connectionless communication. It does not establish a connection before sending data, thus reducing the time it takes to send packets across the network.

3. Open Shortest Path First (OSPF)
   OSPF is an internal routing protocol used within the offices to manage the routing of data between different segments of the network. It is a link-state routing protocol that ensures dynamic routing by calculating the shortest path based on various network metrics like bandwidth and link cost.

   - Justification: OSPF is chosen because it supports scalability and fast convergence. As the company grows and adds more offices or departments, OSPF can dynamically adjust routing tables to reflect changes in the network. Additionally, OSPF allows for hierarchical routing, which is beneficial for large networks as it reduces the size of routing tables and improves overall performance.

   - Data Communication Principles: OSPF is based on the link-state algorithm. Each router in an OSPF network maintains a topology map of the network, which helps routers make more informed decisions about how to route data. OSPF uses cost as its metric, which typically correlates with the bandwidth of the links.

4. IP Security (IPsec)
   IPsec is a suite of protocols used for securing network communications by authenticating and encrypting each IP packet within a communication session. It is used for VPN connections between the Dhaka and Chattogram offices and for remote developer access to ensure data confidentiality, integrity, and authentication.

   - Justification: IPsec ensures that sensitive business data remains secure as it travels over public networks (e.g., the internet). It provides robust encryption (e.g., AES-256) and secure authentication mechanisms, protecting the data from unauthorized access and tampering.

   - Data Communication Principles: IPsec operates at the network layer and uses cryptographic methods to ensure security. It provides confidentiality through encryption, integrity by ensuring that data has not been altered, and authentication to verify the identity of communicating parties. IPsec also supports secure tunneling for remote access.

Access Methods

1. Wired Ethernet
   Wired Ethernet is used for devices within the offices that require stable and high-speed connectivity. This method ensures that devices such as desktops, servers, and workstations can communicate without interruptions. Ethernet offers high throughput and low latency, making it ideal for critical business operations.

    - Justification: Ethernet provides a reliable, low-latency connection and high bandwidth, making it essential for office operations. Ethernet's cost-effectiveness and scalability also make it ideal for expanding office networks as the company grows.

2. Wireless (Wi-Fi)
   Wireless access is implemented using Wi-Fi, which allows employees to work from anywhere within the office without being tied to a physical connection. Wi-Fi is also provided for guest users, with a separate SSID to maintain network security.

    - Justification: Wi-Fi ensures that employees have flexibility within the office, allowing for mobility while maintaining a stable connection to network resources. It supports both 2.4 GHz and 5 GHz frequencies to balance range and speed.

Addressing Models

1. IPv4
   IPv4 is used primarily because it is widely compatible with existing infrastructure and devices. It provides enough IP address space for the current needs of the company.
    - Justification: IPv4 is compatible with almost all network devices and services, making it the preferred addressing model for internal communications.
2. IPv6
   IPv6 is planned for future scalability, as the IPv4 address space becomes more limited. IPv6 offers a much larger address pool and supports more efficient routing.
    - Justification: As the company grows and requires more devices on the network, IPv6 will provide the necessary address space and future-proofing for the network.
3. Dual-Stack
   The dual-stack approach uses both IPv4 and IPv6 to ensure compatibility with legacy systems while allowing for IPv6 adoption as the network grows.
    - Justification: The dual-stack model ensures that both new and legacy devices can operate in parallel. As the transition to IPv6 continues, this approach ensures that the network remains fully functional and compatible with all systems.

4. Network Design and Diagram for Inspire IT Solutions

Physical Layout

The physical layout of the network includes the devices, routers, switches, wireless access points, and the connections between the Dhaka office, Chattogram office, and remote developers.

1. Dhaka Office (Headquarters):
    - Routers: A router is deployed to connect the office to the internet and the Chattogram office via a site-to-site VPN. Another router handles inter-department communication within the office.
    - Switches: Multiple switches are used to connect various devices (workstations, printers, servers) in different departments.
    - Wireless Access Points (APs): APs are placed in various parts of the office to provide Wi-Fi connectivity to employees.
    - Firewall: A firewall is used to secure internal resources and prevent unauthorized access.
2. Chattogram Office (Branch):
    - Similar to the Dhaka office, there is a router and switches for internal communication.
    - Wireless Access Points are used for employee mobility within the office.
    - The site-to-site VPN links the Chattogram office to the Dhaka office, providing secure communication between them.
3. Remote Developers:
    - Remote developers are connected via VPN clients installed on their devices. They securely connect to the Dhaka office's internal network over the public internet.
    - These connections are secured using IPsec VPN, ensuring encrypted and safe communication.

Logical Layout

The **logical layout** focuses on how the network is structured to handle traffic, security, and efficiency.

1. **VLANs (Virtual Local Area Networks)**:
    - VLANs are used to logically segment the network and ensure the security and efficient use of bandwidth within the office environment.
    - Dhaka Office VLANs:
        - Admin VLAN: Dedicated to the administrative staff, isolated from other departments.
        - Development VLAN: Used by developers to maintain data privacy and high-performance communication.
        - Testing VLAN: Used by the testing team to isolate traffic related to the testing environment.
        - Sales & Marketing VLAN: Used by the sales and marketing departments to ensure that their data does not interfere with other departments.
        - Customer Support VLAN: Dedicated to support staff for managing customer-facing applications.
    - Chattogram Office VLANs: Similar VLAN configurations as in Dhaka, ensuring the departments in Chattogram are segregated.
2. **Routing Methods**:
    - OSPF (Open Shortest Path First): An interior gateway protocol is used for dynamic routing within the office networks. OSPF ensures that if any part of the network goes down or changes, routers can dynamically adapt and find the best route for traffic. This is crucial for both Dhaka and Chattogram offices, ensuring efficient communication between different departments.
    - Static Routing: For the inter-office VPN connection, static routes are configured to ensure the traffic between the two offices takes the VPN tunnel.

3. **Wireless Access Points (APs)**:

    - Access Points (APs) provide Wi-Fi connectivity within both office locations. APs are strategically placed to ensure full coverage, allowing employees to move around the office without losing their connection.
    - SSID Configuration:
        - Employee SSID: For authorized users (employees) to connect to the internal network.
        - Guest SSID: For visitors and temporary access, which is isolated from the internal network for security.
        - The APs operate on both **2.4 GHz** (longer range, suitable for low-bandwidth applications) and **5 GHz** (shorter range but higher speeds, ideal for high-performance applications).

Inter-office and Remote Developer Integration

1. **Inter-office Integration**:

    - The **Dhaka** and **Chattogram offices** are connected via a site-to-site VPN. This VPN connection ensures that both offices can securely communicate over the internet, accessing shared resources like file servers, databases, and internal applications.
    - **IPsec (Internet Protocol Security)** is used for VPN encryption, ensuring that all data transferred between the two offices remains confidential and protected from unauthorized access.
    - **Routing Between Offices**: The OSPF routing protocol helps the routers in both offices dynamically share information about network topology and automatically adjust routes when changes occur, ensuring efficient data flow between the two locations.

2. **Remote Developer Integration**:

   - Remote developers are connected to the Dhaka office network via a client-based VPN, using IPsec VPN to ensure secure, encrypted communication.
   - The VPN client on each developer's device authenticates the user and establishes a secure tunnel for data transmission. This allows the developers to access internal resources, including databases, servers, and applications hosted at the Dhaka office.
   - **Multi-factor authentication (MFA)** is enforced for remote access to ensure that only authorized personnel can connect to the internal network.

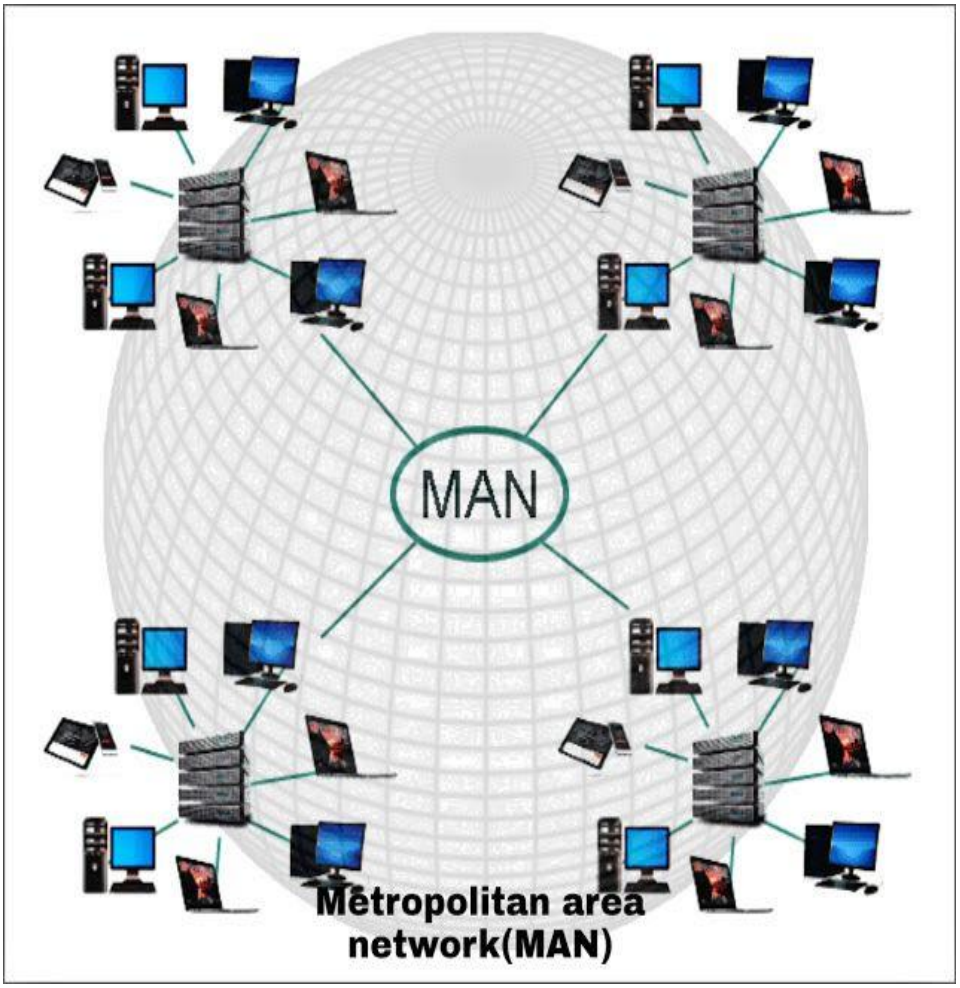

Figure 1: Network Pattern for the IT Company

5. IP Addressing and Subnetting Plan

In this section, we define the IP address allocation for Inspire IT Solutions. The addressing plan will ensure that each department in both the Dhaka and Chattogram offices has its own distinct range, facilitating VLANs, network segmentation, and security. This plan also accommodates future growth by providing enough IP addresses for new devices and employees over the next two years.

IP Address Allocation Table

Below is the IP address allocation for each department in both offices. The plan uses VLSM (Variable Length Subnet Masking) to maximize the use of available IP addresses while accommodating the required number of devices for each department.

Department	Subnet Mask	IP Range	Gateway
Admin (Dhaka)	255.255.255.0	192.168.1.0 - 192.168.1.255	192.168.1.1
Development (Dhaka)	255.255.255.0	192.168.2.0 - 192.168.2.255	192.168.2.1
Testing (Dhaka)	255.255.255.0	192.168.3.0 - 192.168.3.255	192.168.3.1
Sales & Marketing	255.255.255.0	192.168.4.0 - 192.168.4.255	192.168.4.1
Customer Support	255.255.255.0	192.168.5.0 - 192.168.5.255	192.168.5.1
Admin (Chattogram)	255.255.255.0	192.168.6.0 - 192.168.6.255	192.168.6.1
Development (Chattogram)	255.255.255.0	192.168.7.0 - 192.168.7.255	192.168.7.1
Testing (Chattogram)	255.255.255.0	192.168.8.0 - 192.168.8.255	192.168.8.1
Remote Developers	255.255.255.0	192.168.9.0 - 192.168.9.255	192.168.9.1

Justification for IP Addressing

- IPv4 Addressing: IPv4 is selected due to its widespread compatibility and ease of implementation with existing network infrastructure. It provides sufficient address space (approximately 4 billion addresses), which is more than enough for the current and future needs of Inspire IT Solutions.
    - Justification for IPv4: IPv4 is still the dominant addressing system in most organizations, and all the required network devices and services support it. Since the company's current needs are met with IPv4, and IPv6 adoption is not critical yet, IPv4 remains the optimal choice.

- IPv6 Considerations: IPv6 is not currently essential for the company but is considered for future scalability. As more devices are connected to the network, the address space in IPv4 may eventually become insufficient. IPv6 provides an incredibly large address space (approximately 340 undecillion addresses), ensuring the company can expand its network without facing address shortages.
    - Justification for IPv6 (Long-Term): While IPv4 addresses are sufficient for now, IPv6 will be adopted as the company grows and additional devices are added. IPv6 will provide flexibility, future-proofing the network infrastructure and simplifying network management in the long run.
- Dual-Stack: The dual-stack model, which uses both IPv4 and IPv6, could be employed as the company gradually transitions to IPv6. This approach will allow for compatibility with both newer devices (supporting IPv6) and legacy devices that still rely on IPv4.
    - Justification for Dual-Stack: Dual-stack allows the company to leverage the benefits of both IPv4 and IPv6 without disruption. As the company scales, dual-stack will allow for a smooth transition to IPv6 while maintaining backward compatibility with IPv4 devices and services.

Subnetting Plan

The subnetting plan ensures efficient IP address allocation, with the following considerations:

- Each department is allocated its own VLAN and subnet to logically separate network traffic. This reduces congestion and enhances security by isolating sensitive data within departments.
- The subnet mask 255.255.255.0 is used for all VLANs, allowing for up to 254 devices per subnet.
- The gateway IP addresses for each department are configured to route traffic within their respective VLANs and to the external network via the router.

This plan supports future scalability, with the ability to expand IP ranges and introduce new subnets as the company grows.

6. Secure Inter-Office and Remote Access Design

In this section, we'll describe how Inspire IT Solutions ensures secure communication between its offices and remote developers. We will focus on the inter-office link, VPN configuration, and remote access controls.

Inter-Office Link and Protocol

Inter-office Connectivity between the Dhaka Office and the Chattogram Office is established using a site-to-site VPN (Virtual Private Network). This ensures that all data transferred between the two offices is encrypted and secure, providing a safe communication channel over the public internet.

Protocol Used: IPsec VPN

- **IPsec** (Internet Protocol Security) is used to create a secure tunnel between the routers in the Dhaka and Chattogram offices.
- **IPsec VPN** offers the following benefits:
    - **Encryption**: All data transmitted between the two offices is encrypted, ensuring confidentiality.
    - **Data Integrity**: The data is validated to ensure that it has not been altered or tampered with during transmission.
    - **Authentication**: Both routers authenticate each other to prevent unauthorized access to the network.

Site-to-Site VPN Configuration

1. **IPsec VPN Configuration**:
    - Both routers in the Dhaka and Chattogram offices are configured to initiate and maintain the VPN connection.
    - Public IP addresses of both routers are used to establish the tunnel.
2. **VPN Tunnel Setup**:
    - The **VPN tunnel** will allow both offices to securely communicate and access shared resources, such as file servers and applications.
    - Routers in both offices will have static routes or OSPF configured to route traffic through the VPN.
3. **VPN Settings**:
    - **Encryption**: AES (Advanced Encryption Standard) with 256-bit keys for strong encryption.
    - **Authentication**: Pre-shared keys (PSK) or digital certificates to authenticate the routers and establish the tunnel.
    - **IKE (Internet Key Exchange)**: Used to negotiate and establish secure communication between the two routers.

Step-by-Step VPN Configuration (Pseudocode)

Here is a simplified pseudocode for setting up the IPsec VPN between the two routers (Dhaka Router and Chattogram Router):

1. Define VPN Parameters:
    - Set the pre-shared key (PSK) for authentication.
    - Define the encryption algorithm (e.g., AES-256).
    - Define the hashing algorithm (e.g., SHA-256).
    - Define the DH group for key exchange (e.g., Group 14).

2. Dhaka Router Configuration (Router 1):

```
peer 192.168.1.2
set encryption aes-256
set authentication sha256
set psk "sharedkey123"
set ipsec policy transform-set ESP-AES256-SHA256
set ipsec peer 192.168.1.2
set local-address 192.168.1.1
set remote-address 192.168.1.2
set tunnel 1
```

3. Chattogram Router Configuration (Router 2):

    - peer 192.168.1.1
    - set encryption aes-256
    - set authentication sha256
    - set psk "sharedkey123"
    - # Configure the IPSec policy
    - set ipsec policy transform-set ESP-AES256-SHA256
    - set ipsec peer 192.168.1.1
    - set local-address 192.168.1.2
    - set remote-address 192.168.1.1
    - set tunnel 1

4. Verify VPN Tunnel

    - Ensure the VPN tunnel is established by using the show crypto ipsec sa command on both routers to check the status

Remote Access Controls for Developers

Remote access allows employees to securely connect to the company's internal resources, regardless of their location. For remote developers, a VPN client is used to establish a secure connection to the Dhaka office network. The IPsec VPN provides the necessary encryption and security for remote communication.

Remote Developer VPN Configuration

1. VPN Client Setup:
    - Developers install the VPN client software (e.g., Cisco AnyConnect) on their laptops or devices.
    - The client is configured with the VPN server IP address (public IP of the Dhaka office router) and the pre-shared key (PSK).
2. Authentication:
    - Multi-factor authentication (MFA) is enforced to ensure that only authorized developers can access the internal network.
    - Developers must authenticate using their username, password, and an additional security token (e.g., a one-time password sent via SMS or email).
3. IP Address Assignment:
    - Upon successful authentication, the VPN server assigns a private IP address (within the Remote Developer VLAN subnet) to the client.
    - The remote developer's device behaves as if it is physically located in the Dhaka office, allowing access to internal resources like file servers, development tools, and databases.
4. Access Control Lists (ACLs):
    - ACLs are configured on the router and firewall to control which resources remote developers can access. For instance:
        - Developers may be allowed to access only the Development and Testing VLANs.
        - Access to sensitive data in the Admin VLAN may be restricted.
    - The firewall rules block unauthorized traffic and ensure that only VPN traffic is allowed.

7. Network Security Architecture

1. Firewall Rules

Firewalls are deployed at strategic points in the network to protect internal resources and prevent unauthorized access from external or internal threats.

Firewall Configuration Overview:

Rule Number	Source	Destination	Service	Action	Description
Rule 1	Internal network (VLANs)	External (Internet)	HTTP, HTTPS, DNS	Allow	Allow standard web traffic from internal network to the internet.
Rule 2	External (Internet)	Internal network (VLANs)	HTTP, HTTPS, DNS	Allow	Allow inbound web traffic (public website).
Rule 3	Remote Developers	Internal network (Development VLAN)	All services (TCP/UDP)	Allow	Allow remote developers to access the development network after successful authentication.
Rule 4	Remote Developers	Internal network (Admin VLAN)	All services (TCP/UDP)	Deny	Block remote developers from accessing administrative services.
Rule 5	Internal network (Admin VLAN)	External (Internet)	SSH, RDP	Allow	Allow administrative access to remote servers via SSH or RDP.
Rule 6	Internal network (All VLANs)	External (Internet)	ICMP (Ping)	Deny	Block ping requests from external sources to prevent network scanning.
Rule 7	Internal network (All VLANs)	Internal network (All VLANs)	All services (TCP/UDP)	Allow	Allow all internal network communication between VLANs.

Explanation:

- Outbound traffic (from internal to external) is allowed for standard services like HTTP, HTTPS, and DNS.
- Inbound traffic (from external to internal) is restricted based on the need for external access, e.g., for a public-facing web server.

- Remote developers can access the Development VLAN but are restricted from accessing sensitive Admin VLAN resources.
- Internal communication between departments (VLANs) is allowed, but external communication is carefully controlled.

2. Access Control Policies

Access control policies help define who can access what within the network. These policies are enforced using technologies like ACLs (Access Control Lists), firewall rules, and VPN settings.

Access Control Policy Overview:

Entity/Role	Access Rights	Description
Admin Users	Full access to Admin VLAN, Testing VLAN, and Development VLAN	Admin users have access to all resources, including servers and applications.
Development Team	Access to Development VLAN, Testing VLAN only	Developers can access resources within the Development VLAN for their work, and testing resources for testing their code.
Customer Support Team	Access to Customer Support VLAN only	Customer support staff can only access customer-facing services and support tools.
Remote Developers	Access to Development VLAN and Testing VLAN only	Remote developers can access development tools, but sensitive data in Admin VLAN is blocked.
Sales and Marketing Team	Access to Sales & Marketing VLAN only	The sales team can only access marketing tools and client-facing resources.
General Employees	Access to General Internal Resources (Admin, Development, Testing, Sales)	Employees who are not in specialized roles can access basic company resources like internal applications.

Explanation:

- Role-based Access Control (RBAC) is implemented, where users are granted access based on their roles.
- VLANs are used to enforce access control policies, ensuring that only authorized personnel can access sensitive resources.
- Remote access is strictly controlled via VPN with multi-factor authentication (MFA) for added security.

3. VLAN Segmentation for Security

VLAN segmentation helps separate traffic between departments, improving both performance and security by ensuring that sensitive data is isolated from other parts of the network. Each department's traffic is isolated into its own VLAN, with appropriate firewall and ACL rules to control access.

VLAN Structure:

- Admin VLAN: Contains administrative resources and should be isolated from other departments.
- Development VLAN: Includes development servers, databases, and tools, isolated from other VLANs for security.
- Testing VLAN: Used for testing environments, ensuring that testing activities do not impact the production network.
- Sales & Marketing VLAN: Segregated to handle marketing tools, customer information, and public-facing applications.
- Customer Support VLAN: Dedicated to customer support systems, preventing unauthorized access to sensitive backend data.
- Remote Developers VLAN: Ensures secure access for remote workers, with controlled access to the Development and Testing VLANs only.

VLAN Benefits:

- Security: Sensitive data is protected by isolating departments into separate VLANs, reducing the risk of unauthorized access.
- Network Efficiency: Reduces broadcast traffic by isolating traffic within each VLAN.
- Easier Management: Network resources can be managed more effectively by assigning different policies to each VLAN.

4. IPS/IDS (Intrusion Prevention/Detection Systems)

Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) are deployed to monitor and protect the network from malicious activities and attacks.

IPS/IDS Configuration:

- IPS: Detects and prevents malicious activities, such as DoS (Denial of Service) attacks, and blocks harmful traffic in real-time.
- IDS: Monitors traffic and generates alerts when it detects suspicious activities, but does not actively block the traffic.

Deployment Locations:

- IPS/IDS at the perimeter of the network (firewall/router level) to monitor all incoming and outgoing traffic.
- IPS/IDS on key servers and internal network segments to detect internal threats.

Example Use Case:

- The IPS can block incoming DDoS (Distributed Denial of Service) attacks targeting the network.
- IDS can send alerts if there is any unusual activity, like excessive login attempts from an IP address, signaling a potential brute-force attack.

5. Authentication Methods

To ensure that only authorized users can access sensitive resources, **authentication** is an essential part of the network's security architecture.

Proposed Authentication Method: RADIUS, Certificates, and 2FA:

- RADIUS (Remote Authentication Dial-In User Service): RADIUS is used to centralize authentication for remote users and devices, ensuring that only authorized users can access the network. RADIUS servers authenticate users trying to access the network by verifying their credentials.
- Certificates: Digital Certificates are used for encrypting communication between devices, ensuring that only authorized devices can communicate over the network. Certificates provide secure device authentication (especially useful for VPN and wireless networks).
- Two-Factor Authentication (2FA): 2FA is implemented for remote access to the network. It requires remote users to provide two forms of authentication:
    1. Something they know: Their username and password.
    2. Something they have: A security token or one-time password (OTP) sent via an app or SMS.

This method adds an extra layer of security by ensuring that even if a password is compromised, an attacker cannot access the network without the second form of authentication.

8. Wireless Network Setup

1. AP Placement Diagram and Rationale

AP Placement is critical for ensuring that the network provides adequate coverage and capacity while avoiding interference and maintaining optimal performance. The placement of Wireless Access Points (APs) is done considering office layout, the number of employees, and potential interference sources.

Placement Diagram Overview:

- Dhaka Office:
    - APs are placed at strategic locations to cover the entire office floor.
    - Multiple APs are placed near key areas like the Development Department, Testing Department, Admin Department, and meeting rooms to ensure seamless Wi-Fi access.
- Chattogram Office:
    - APs are also placed at key locations, ensuring full coverage for employees working across the office.
    - Locations like conference rooms, lobby areas, and common spaces are given high priority for Wi-Fi coverage.

Rationale for AP Placement:

- Signal Coverage: APs should be placed in locations that allow the signals to cover the entire office space without overlapping excessively to avoid interference.
- Traffic Load: APs are placed in areas with higher traffic (e.g., development teams, meeting rooms) to ensure that there is sufficient bandwidth and minimal congestion.
- Minimized Interference: Avoid placing APs near heavy electronic equipment (e.g., printers, large metal objects) that could cause interference.
- Redundancy: Multiple APs ensure that if one fails, others can continue to provide coverage, maintaining a high level of availability.

2. SSID Naming and Segmentation

To improve network security and manageability, the wireless network is segmented into different SSIDs (Service Set Identifiers) based on the type of users (employees, guests). Each SSID will have its own security settings to ensure that internal network resources are protected.

SSID Configuration:

- **Employee SSID**:
  - SSID Name: `Inspire_IT_Employees`
  - Purpose: For authorized employees to access the internal network and resources.
  - Security: WPA3 encryption for strong security. Username/password authentication, with 2FA (Two-Factor Authentication) for additional security.
- **Guest SSID**:
  - SSID Name: `Inspire_IT_Guests`
  - Purpose: For guests and visitors who require internet access without accessing internal company resources.
  - Security: WPA2 encryption for secure access. The guest network is isolated from the internal network using VLANs and firewall rules.
  - Network Isolation: Traffic from the guest network is segregated from the internal network via VLAN segmentation and firewall rules to prevent access to internal company resources.

Segmentation Rationale:

- Employee SSID is reserved for internal employees to access critical business systems, file servers, and communication tools.
- Guest SSID is designed to provide internet access only to visitors, without granting access to any of the internal company's resources.

3. Channel Planning (2.4GHz/5GHz)

Proper channel planning is essential to ensure minimal interference and optimize the performance of the wireless network. By using both 2.4GHz and 5GHz frequency bands, we can take advantage of the different range and capacity characteristics of each band.

2.4GHz Channel Planning:

- Advantages: The 2.4GHz band provides longer range and better penetration through walls and other obstacles. However, it is more congested due to the number of devices using the same spectrum (e.g., microwaves, Bluetooth devices).
- Channel Selection: In the 2.4GHz band, there are only 3 non-overlapping channels: Channel 1, Channel 6, and Channel 11. These channels should be used to minimize interference.
  - AP 1: Channel 1
  - AP 2: Channel 6
  - AP 3: Channel 11

5GHz Channel Planning:

- Advantages: The 5GHz band provides higher speeds and less interference compared to 2.4GHz. However, it has a shorter range and does not penetrate obstacles as effectively.
- Channel Selection: The 5GHz band offers a much larger number of non-overlapping channels, which allows for more flexible and interference-free channel assignment.
    - Channels like 36, 40, 44, 48, 149, 153, 157, 161, etc., can be assigned to APs based on the placement and interference levels.
    - AP 1: Channel 36
    - AP 2: Channel 40
    - AP 3: Channel 44

Channel Planning Rationale:

- 2.4GHz is used for general coverage and devices that require long-range access but do not need high-speed internet.
- 5GHz is used for high-performance applications such as video conferencing, large file transfers, and real-time development tasks, as it provides higher speeds and lower interference.

9. Optimization and Monitoring Plan

1. Quality of Service (QoS) Setup for Prioritizing Services

Quality of Service (QoS) is essential for ensuring that critical applications and services receive the necessary bandwidth and low latency, while less important traffic (such as general browsing or non-business-related applications) does not affect the performance of high-priority services.

QoS Configuration and Prioritization:

- Voice and Video Traffic: The highest priority should be given to VoIP (Voice over IP) and video conferencing traffic, as these are real-time applications that are sensitive to delays and packet loss.
    - Class of Service (CoS): Assign CoS 5 (highest priority) to VoIP and video traffic.
    - Traffic Shaping: Implement traffic shaping to limit the bandwidth for non-critical traffic, ensuring enough bandwidth for VoIP and video.

- Development and Testing Traffic: Development tools, version control systems, and test environments must be given priority over less critical traffic (such as general web browsing).
- General Office Traffic: Internal data transfer and web traffic can be assigned CoS 3 or lower, ensuring that normal office operations run smoothly without affecting high-priority services.

QoS Traffic Classification:

- VoIP and Video Traffic: CoS 5
- Development and Testing Traffic: CoS 4
- General Office Traffic: CoS 3 or lower
- Guest Traffic: CoS 2 (lowest priority)

By implementing **QoS**, the company can ensure that critical services, such as video conferences, are not disrupted by network congestion or delays.

2. Monitoring Tools

To ensure the network operates smoothly, monitoring tools are critical. These tools help track network performance, availability, and detect issues before they become critical.

Recommended Monitoring Tools:

- **PRTG Network Monitor**:
    - PRTG is an all-in-one monitoring solution that can track the performance of network devices, bandwidth usage, and application performance.
    - Key Features: It offers real-time monitoring of network traffic, alerts for bottlenecks, device status, and monitoring VPN connections.
    - Usage: PRTG can be used to monitor QoS, VPN traffic, VLANs, routers, and APs for any signs of performance degradation.
- **SNMP (Simple Network Management Protocol)**:
    - SNMP is widely used for network monitoring and management. It allows network devices like routers, switches, and firewalls to communicate their status to a central monitoring system.
    - Usage: SNMP can be configured to track device health, bandwidth usage, CPU load, and memory utilization across the network. It is essential for monitoring the performance of routers and switches.

- **Wireshark**:
    - Wireshark is a packet analyzer used to monitor network traffic at the packet level.
    - Usage: This tool is helpful for troubleshooting network issues, such as latency or packet loss, and analyzing network performance in-depth.

Centralized Dashboard:

- Combine PRTG, SNMP, and Wireshark into a **centralized dashboard** to give network administrators a clear overview of the health of the network, including real-time alerts on traffic, device status, and critical events.

3. Scalability Plan (20% Device Growth)

As Inspire IT Solutions grows, the network will need to handle an increase in devices and users, estimated at 20% growth in the next two years. Here is how scalability will be addressed:

Scalability Considerations:

- **IP Addressing**:
    - The current IP addressing plan is designed to accommodate future growth by reserving sufficient address space in each VLAN. The use of VLSM (Variable Length Subnet Masking) allows for flexible subnetting to accommodate the growing number of devices without wasting IP addresses.
    - IPv6 Adoption: While IPv4 is sufficient for now, IPv6 should be considered as the company expands, as it provides an almost unlimited pool of IP addresses.
- **Device Capacity**:
    - Switches and Routers: The current network infrastructure, including switches and routers, will support growth by ensuring that new devices can be added with minimal disruption. Modular switches and stackable routers can be added as the demand for bandwidth increases.
    - Access Points (APs): As the number of users and devices increases, more APs will be added to handle the additional load. Wireless Controller devices can be used to manage and configure multiple APs centrally.
- **Bandwidth Planning**:
    - The core network links should be designed with sufficient bandwidth to handle future traffic increases. Ethernet connections with 1 Gbps or 10 Gbps links should be used for internal communication, and VPN bandwidth should be adjusted as more remote workers are added.

- **Cloud Services and Virtualization**:
    - As the company grows, transitioning to cloud-based services for file storage, application hosting, and other infrastructure will reduce the burden on on-premise devices and simplify the scaling of network resources.

4. Bottleneck Detection Methods

Detecting **bottlenecks** in the network is essential to maintaining high performance. Common bottlenecks include insufficient bandwidth, overloaded routers or switches, and misconfigured devices.

Bottleneck Detection Methods:

- Bandwidth Utilization Monitoring: Using PRTG or SNMP, monitor the bandwidth usage on key network links (such as between offices, internal departments, and remote access VPN). If a link is consistently near full utilization, this indicates a potential bottleneck.
- Latency and Packet Loss: Use Wireshark or PRTG to monitor for latency spikes or packet loss on critical network paths. These issues can indicate overloaded devices or misconfigured network settings.
- Router and Switch CPU Utilization: Router and switch CPU usage can be monitored to identify if these devices are overburdened. If CPU utilization is consistently high, it may indicate a bottleneck, and the devices may need upgrading or reconfiguration.
- Flow Monitoring: Using NetFlow or sFlow, monitor traffic patterns and identify high traffic sources that could be causing congestion. This helps pinpoint whether a specific application or service is consuming excessive bandwidth.
- Real-Time Alerts: PRTG can be configured to send real-time alerts when a threshold is exceeded, indicating a potential bottleneck.

10. Conclusion and Reflection

The network design for Inspire IT Solutions ensures that the company's infrastructure is secure, efficient, and scalable. The design considers both current needs and future growth, providing a robust framework for day-to-day operations and for adapting to the increasing demands of the business. This section summarizes the system's strengths, discusses compromises made between security and performance, and reflects on potential issues that could arise, along with the mitigation strategies.

System's Strengths

1. **Security and Integrity**:
   The design prioritizes security with the implementation of IPsec VPN for both inter-office and remote access communication. VLAN segmentation isolates sensitive data and ensures that internal resources are protected from unauthorized access. Additionally, firewall rules and access control policies are put in place to filter traffic, limiting exposure to potential threats.

2. **Scalability**:
   The network is built to scale with a projected 20% device growth in the coming years. The IP addressing scheme uses VLSM, and the network can easily accommodate additional devices without requiring significant changes to the infrastructure. The use of dual-stack IP ensures compatibility with both IPv4 and IPv6, allowing for smoother future transitions as more devices are added to the network.

3. **Performance and Efficiency**:
   QoS (Quality of Service) has been implemented to prioritize time-sensitive traffic, such as VoIP and video conferencing, ensuring that these applications perform optimally even in peak usage periods. The network design ensures that employees have access to the necessary resources with minimal latency, whether in the office or working remotely.

4. **Redundancy and Reliability**:
   The VPN and firewall configurations include redundancy to ensure high availability. The network is designed with failover mechanisms to protect against outages, ensuring that critical business operations remain unaffected during any hardware failures.

5. **Centralized Monitoring**:
   The use of PRTG Network Monitor and SNMP enables centralized monitoring of the network's health, bandwidth usage, and device performance. This allows network administrators to detect issues early and take action before they impact business operations.

Compromises Made

1. **Security vs. Performance**:
   In many network designs, a trade-off exists between security and performance. For Inspire IT Solutions, while IPsec VPNs provide strong encryption for secure communication, they can introduce latency and reduce the network's throughput. However, this compromise is justified due to the importance of data confidentiality and the need to protect sensitive business information, especially when employees are working remotely or connecting between offices.

2. **Access Control vs. Convenience**:
   The strict access control policies, which limit access to certain VLANs and resources, can introduce some inconvenience for employees who may require cross-departmental access. However, these policies were necessary to ensure that sensitive data within the Admin VLAN and Development VLAN is protected from unauthorized access, especially from remote developers or other departments.

3. **Guest Network Segmentation vs. Usability**:
   The Guest SSID is isolated from the internal network for security reasons. While this ensures data privacy and protects internal resources from guest access, it may create inconvenience for visitors who need to access internal resources. In this case, balancing convenience and security was essential, and providing a secure and isolated network for guests was prioritized.

Potential Issues and Mitigations

1. **VPN Performance Overhead**:
   One potential issue with using IPsec VPNs for inter-office and remote access is the performance overhead caused by encryption and decryption processes. This could result in increased latency and slower connection speeds for remote workers.

   - Mitigation: To address this, the VPN configuration can be optimized by using hardware-accelerated encryption devices, and the network can be monitored using PRTG to identify any bottlenecks. Additionally, high-bandwidth VPN tunnels can be deployed between offices to ensure fast communication.

2. **Network Congestion**:
   High traffic volumes in certain parts of the network could lead to congestion, particularly in VLANs that handle more data-intensive applications, such as the Development VLAN. This could lead to a degraded user experience for developers or other users accessing large files or cloud-based applications.

    - Mitigation: The use of QoS ensures that time-sensitive traffic like VoIP and video conferencing has higher priority. For non-critical applications, such as file sharing, the network should have load balancing and traffic shaping mechanisms in place to prevent congestion during peak hours.

3. **Scalability Limitations in APs**:
   As the number of employees grows, wireless connectivity may become an issue, particularly in areas with high device density. The current number of APs may not suffice to handle the increased demand.

    - Mitigation: The wireless network design incorporates multiple APs placed in key locations, with careful attention to channel planning to avoid interference. Additional APs can be added as the company grows. The use of wireless controllers will help in managing multiple APs to ensure consistent coverage and performance.

4. **Human Error in Configuration**:
   With complex configurations (e.g., VPNs, firewall rules, and VLAN setups), human error in network configuration could lead to misconfigurations, causing downtime or security vulnerabilities.

    - Mitigation: To reduce human error, automated configuration management tools like Ansible or Cisco DNA Center should be employed. Additionally, regular network audits and configuration reviews should be conducted to ensure the network remains properly configured.

5. **Over-reliance on External VPN Connectivity**:
   Remote access heavily relies on VPN connections, which could be vulnerable to internet connectivity issues or DDoS attacks.

    - Mitigation: A redundant VPN setup can be implemented, using multiple internet connections (e.g., using MPLS alongside VPN) to ensure reliable communication. Additionally, intrusion prevention systems (IPS) and DDoS protection can be implemented to safeguard remote access connections.

References

1. J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, 7th ed., Pearson, 2017.
2. J. Postel, "Internet Protocol," RFC 791, 1981. [Online]. Available: https://tools.ietf.org/html/rfc791. [Accessed: Aug. 15, 2021].
3. W. Stallings, *Network Security Essentials: Applications and Standards*, 6th ed., Pearson, 2017.
4. SolarWinds, *PRTG Network Monitor*. [Online]. Available: https://www.solarwinds.com. [Accessed: Aug. 15, 2021].
5. Cisco, *Cisco AnyConnect Secure Mobility Client*, 2020. [Online]. Available: https://www.cisco.com. [Accessed: Aug. 15, 2021].
6. Wireshark, *Wireshark Network Protocol Analyzer*. [Online]. Available: https://www.wireshark.org. [Accessed: Aug. 15, 2021].
7. Ubiquiti Networks, *UniFi Access Points*, 2021. [Online]. Available: https://ui.com/unifi. [Accessed: Aug. 15, 2021].
8. Cisco Systems, *Cisco IOS XR Configuration Guide*, 2021. [Online]. Available: https://www.cisco.com. [Accessed: Aug. 15, 2021].
9. Juniper Networks, *Juniper Networks SRX Series Services Gateways - Security Configuration Guide*, 2020. [Online]. Available: https://www.juniper.net. [Accessed: Aug. 15, 2021].
10. Fortinet, *FortiGate Security Cookbook*, 2021. [Online]. Available: https://www.fortinet.com. [Accessed: Aug. 15, 2021].