Contents

[**Introduction** 2](#_Toc169958827)

[**Discussion** 2](#_Toc169958828)

[**Network Diagram** 2](#_Toc169958829)

[**Specific Interaction: Online Bill Payment via Telstra's Website** 4](#_Toc169958830)

[**Recommendations for Telstra on Data Distribution and Data Safety** 6](#_Toc169958831)

[**Conclusion** 7](#_Toc169958832)

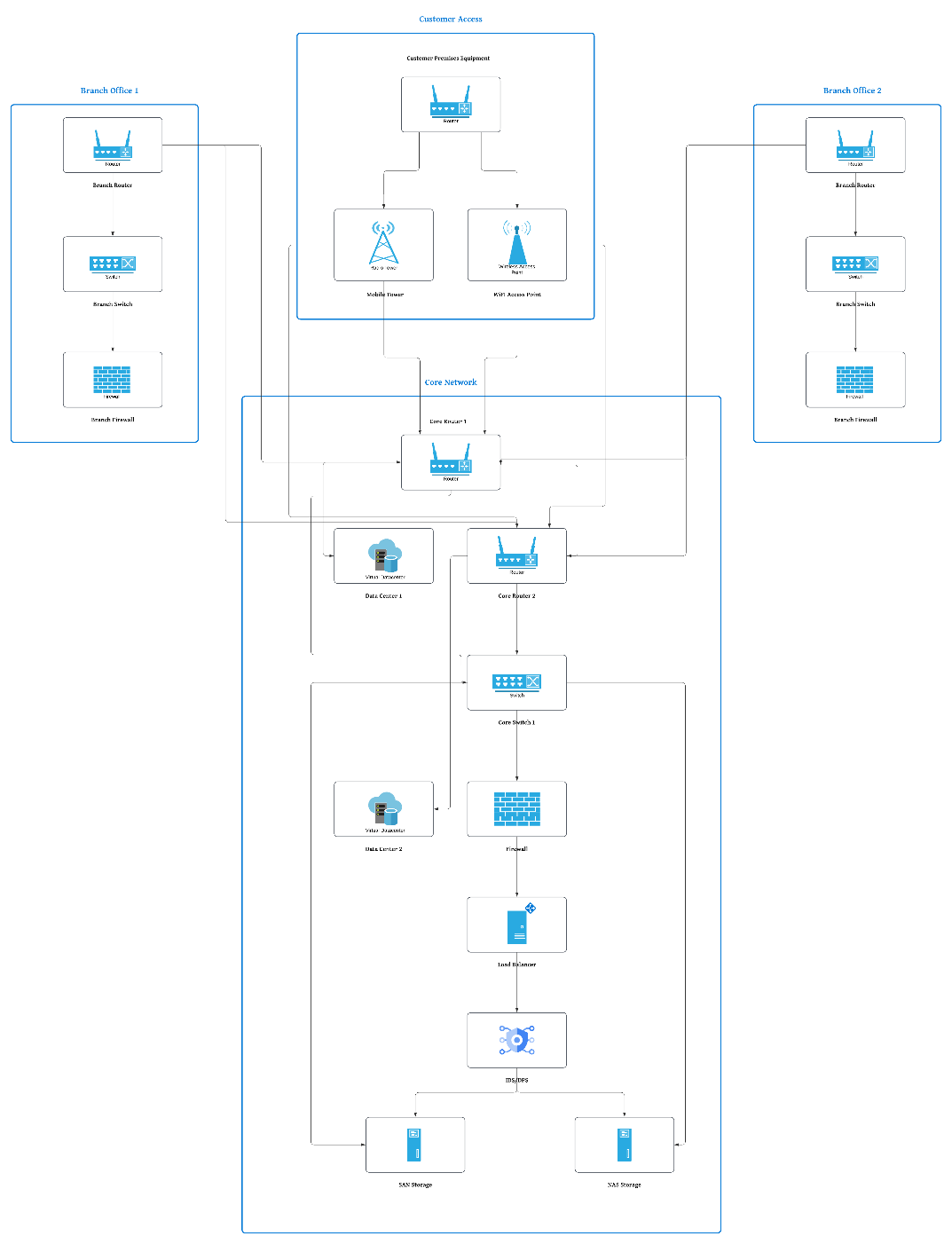
[**References** 8](#_Toc169958833)

# **Introduction**

Telstra is Australia's largest telecommunications and technology company, offering a comprehensive range of communications services, including mobile, internet, and entertainment to both residential and business customers. This report examines Telstra's network infrastructure, focusing on the devices, protocols, and technologies used to ensure efficient data distribution and security. Readers will find a detailed network diagram, an analysis of data transmission during a typical customer interaction, and actionable recommendations for enhancing data safety and network performance.

# **Discussion**

## **Network Diagram**

****

The network diagram for Telstra illustrates the comprehensive infrastructure supporting its operations, focusing on key devices and their roles in data transmission and storage. The main devices and their functionalities within the network are as follows:

1. **Core Network Devices:**
   * Routers: Core Routers (CR1 and CR2) direct data packets across the network, ensuring efficient data routing.
   * Switches: The Core Switch (CS) connects various network segments within the data centers, facilitating internal data flow.
   * Firewalls: Positioned at key points, firewalls (FW) protect the network by filtering incoming and outgoing traffic based on security rules.
   * Load Balancers: Distribute incoming network traffic evenly across multiple servers to optimize resource use and ensure reliability.
   * IDS/IPS: Intrusion Detection and Prevention Systems monitor network traffic for suspicious activities and respond to potential threats.
2. **Data Storage and Access Devices:**
   * Servers: Host various applications, databases, and services essential for Telstra’s operations. These include Web Servers for handling user requests and Database Servers for storing user data and transaction records.
   * SAN Storage: Storage Area Networks provide high-speed access to consolidated block-level data storage, crucial for large-scale data management.
   * NAS Storage: Network Attached Storage offers centralized storage accessible by multiple users over the network, facilitating shared access to data.
3. **Internet Access and Connectivity:**
   * Mobile Towers: Facilitate wireless communication by connecting mobile devices to Telstra’s network, enabling mobile internet access.
   * Wi-Fi Access Points: Provide wireless internet access in designated areas, allowing devices to connect to the network wirelessly.
   * Customer Premises Equipment (CPE): Includes modems and routers located at customer sites, providing connectivity between customer devices and Telstra’s network.
4. **Branch Offices and Departments:**
   * Branch Office Networks: Each branch office is equipped with local routers (BR1, BR2), switches (BS1, BS2), and firewalls (BF1, BF2) to connect securely to the core network.

## **Specific Interaction: Online Bill Payment via Telstra's Website**

For this scenario, we will focus on the interaction between a customer and Telstra’s online bill payment system. The process involves the customer accessing Telstra’s website, entering payment details, and receiving confirmation.

**Devices Involved**

1. **Customer Devices**
   * **Customer Premises Equipment (CPE)**: Modem/router providing internet access.
   * **Customer Device**: Laptop, smartphone, or tablet used to access the website.
2. **Telstra's Network Devices**
   * **Mobile Tower / Wi-Fi Access Point**: Facilitates wireless communication from the customer device to the internet.
   * **Core Router (CR1/CR2)**: Directs data packets within Telstra’s network.
   * **Core Switch (CS)**: Connects different network segments.
   * **Firewall (FW)**: Protects the network from unauthorized access.
   * **Load Balancer (LB)**: Distributes incoming traffic to the appropriate server.
   * **Web Server**: Hosts Telstra’s website and handles user requests.
   * **Database Server**: Stores user data and transaction records.
   * **SAN/NAS Storage**: Provides persistent storage for transaction logs and user data.

**Media Communications Utilized**

1. **Wireless Communication**:
   * **Wi-Fi**: Used by the customer device to connect to the CPE.
   * **4G/5G Cellular Network**: Used if the customer is accessing the website via a mobile network.
2. **Wired Communication**:
   * **Fiber Optic Cables**: Used within Telstra’s backbone network for high-speed data transmission between core network devices and data centers.
   * **Ethernet**: Connects devices within data centers (e.g., servers, switches).

**Data Flow and Protocols**

1. **Customer Access and Data Entry**
   * **HTTP/HTTPS**: The customer accesses Telstra’s website using HTTPS (HyperText Transfer Protocol Secure), which ensures that data transmitted between the customer’s browser and the web server is encrypted and secure.
   * **Protocol Used**: HTTPS (HTTP over SSL/TLS) to secure the data during transmission, ensuring that sensitive information such as payment details are encrypted.
2. **Data Transmission within Telstra's Network**
   * **IP**: The data packets are routed through Telstra’s network using the Internet Protocol (IP), ensuring that they reach the correct destination.
   * **Protocol Used**: IP (Internet Protocol) for addressing and routing data packets across the network.
3. **Server Processing and Database Storage**
   * **TCP**: The Transmission Control Protocol ensures reliable transmission of data packets between the customer’s device and Telstra’s web server.
   * **SQL**: The Structured Query Language is used to interact with the database server, executing commands to store and retrieve transaction data.
   * **Protocol Used**:
     + **TCP (Transmission Control Protocol)**: For reliable communication between devices.
     + **SQL (Structured Query Language)**: For database interactions and data storage.
4. **Data Retrieval and Confirmation**
   * **HTTPS**: Used again to transmit confirmation details back to the customer’s device securely.
   * **SMTP**: If an email confirmation is sent, the Simple Mail Transfer Protocol is used for sending the email.

**Relevant Protocols Discussion**

1. **HTTPS (HyperText Transfer Protocol Secure)**
   * **Usage**: Secures the communication between the customer’s web browser and Telstra’s web server.
   * **Importance**: Ensures that sensitive information, such as payment details, is encrypted and protected from eavesdropping or tampering.
2. **IP (Internet Protocol)**
   * **Usage**: Responsible for addressing and routing packets of data from the customer’s device to the web server and back.
   * **Importance**: Provides the fundamental addressing system that allows data to be sent and received across the internet and within Telstra’s internal network.
3. **TCP (Transmission Control Protocol)**
   * **Usage**: Ensures reliable and ordered delivery of data packets between the customer’s device and Telstra’s servers.
   * **Importance**: Provides error checking and guarantees that data packets are delivered in the correct order, ensuring data integrity and reliability.

## **Recommendations for Telstra on Data Distribution and Data Safety**

1. **Implement Zero Trust Architecture**
   * **Recommendation**: Adopt a Zero Trust security model that requires verification at every stage of the network interaction, regardless of whether the connection is inside or outside the network perimeter.
   * **Actionable Steps**:
     + Implement multi-factor authentication (MFA) for all access points.
     + Continuously monitor and log all network traffic.
     + Use micro-segmentation to limit access to only necessary network resources.
   * **Supporting Reference**: "Zero Trust Security: What It Is, How It Works and Why It Matters" Cisco
2. **Enhance Data Encryption Standards**
   * **Recommendation**: Strengthen data encryption methods both in transit and at rest to ensure data safety against interception and breaches.
   * **Actionable Steps**:
     + Upgrade encryption protocols to TLS 1.3 for all data in transit.
     + Use Advanced Encryption Standard (AES) with 256-bit keys for data at rest.
     + Regularly audit encryption practices and update algorithms as needed.
   * **Supporting Reference**: "Transport Layer Security (TLS) - RFC 8446" IETF
3. **Implement Advanced Threat Detection and Response**
   * **Recommendation**: Deploy advanced threat detection and response systems to proactively identify and mitigate security threats.
   * **Actionable Steps**:
     + Integrate AI-driven security information and event management (SIEM) systems.
     + Use Endpoint Detection and Response (EDR) tools to monitor endpoint activities.
     + Conduct regular penetration testing and vulnerability assessments.
   * **Supporting Reference**: "The Value of an Advanced Threat Detection and Response Solution" Gartner

**Supporting Discussion**

1. **Zero Trust Architecture**: By implementing Zero Trust, Telstra can significantly reduce the risk of unauthorized access and lateral movement within the network. Zero Trust ensures that even if an attacker gains access to one part of the network, they cannot easily move to other areas without re-authentication and verification.
2. **Data Encryption**: Upgrading to TLS 1.3 and using AES-256 for encryption will enhance the security of data both in transit and at rest. TLS 1.3 provides improved security features and performance over previous versions, while AES-256 is widely recognized as one of the most secure encryption standards available.
3. **Advanced Threat Detection**: Advanced threat detection systems, powered by AI and machine learning, can identify unusual patterns and potential threats more effectively than traditional methods. Integrating these tools can help Telstra detect and respond to security incidents in real-time, minimizing potential damage.

These recommendations focus on enhancing Telstra's overall security posture by addressing critical areas in network technology, protocols, and architecture. Implementing these measures will help ensure robust data distribution and safety across the network.

# **Conclusion**

In summary, Telstra's network infrastructure is designed to support its extensive range of telecommunications and technology services. The network is composed of various core devices, including routers, switches, firewalls, and load balancers, which ensure efficient and secure data transmission. Data storage and access are facilitated through SAN and NAS devices, while mobile towers and Wi-Fi access points provide internet connectivity for customers. Our analysis of a typical customer interaction, such as online bill payment, highlighted the crucial roles of protocols like HTTPS, IP, and TCP in ensuring data safety and reliability. Finally, the recommendations provided focus on adopting a Zero Trust architecture, enhancing data encryption standards, and implementing advanced threat detection systems to further improve data distribution and network security. These measures will help Telstra maintain its leadership in delivering reliable and secure telecommunications services.

# **References**

Cisco. (n.d.). Cisco core routers. Cisco. Retrieved from <https://www.cisco.com/c/en/us/products/routers/>

Cloudflare. (n.d.). What is HTTPS? Why use HTTPS? Cloudflare. Retrieved from <https://www.cloudflare.com/learning/ssl/why-use-https/>

Dell Technologies. (n.d.). SAN storage solutions. Dell Technologies. Retrieved from <https://www.delltechnologies.com/en-us/storage/san.htm>

F5 Networks. (n.d.). Load balancers. F5 Networks. Retrieved from <https://www.f5.com/products/big-ip-services/load-balancer>

Fortinet. (n.d.). Firewall security. Fortinet. Retrieved from <https://www.fortinet.com/products/firewall>

GeeksforGeeks. (n.d.). Internet protocol - Introduction. GeeksforGeeks. Retrieved from <https://www.geeksforgeeks.org/internet-protocol/>

Gartner. (2021). The value of an advanced threat detection and response solution. Gartner. Retrieved from <https://www.gartner.com/en/documents/3987488/the-value-of-an-advanced-threat-detection-and-response-solut>

Hewlett Packard Enterprise. (n.d.). Network switches. Hewlett Packard Enterprise. Retrieved from <https://www.hpe.com/us/en/networking/switches.html>

Microsoft. (n.d.). Transmission control protocol (TCP). Microsoft Docs. Retrieved from <https://docs.microsoft.com/en-us/windows/win32/winsock/transmission-control-protocol-tcp>

Synology. (n.d.). NAS storage. Synology. Retrieved from <https://www.synology.com/en-global/products/NAS>

Cisco. (n.d.). Zero trust security: What it is, how it works and why it matters. Cisco. Retrieved from <https://www.cisco.com/c/en/us/products/security/zero-trust-security.html>