**ICTTEN622 Simulation Pack**

**Simulation 1: Aussie Home Essentials**

Aussie Home Essentials is a small retail chain with 3 stores in suburban areas across Brisbane. They are planning to open 2 additional stores over the next year.

**Overall objective:**

The company needs an ICT network architecture design that supports its current operations and can scale to meet future needs. The network should handle basic point-of-sale (POS) systems, inventory management, and internal communication between the stores.

**Business problem:**

Some stores experience slow POS transactions, poor connectivity for inventory management, and frequent downtimes, especially during peak shopping hours. This inconsistency causes delays, frustration among staff, and a poor customer experience.

**Business opportunity:**

A centralised cloud-based network architecture could give all stores consistent access to real-time inventory data, improving stock management and customer satisfaction. A centralised system also simplifies updates, maintenance, and security management, reducing long-term operational costs.

**Budget:** $50,000–$75,000

**Timeline:** 8 weeks

**Details and specifications**

* Existing network type: basic LAN in each store, no centralised WAN.
* Number of users: 45 existing users (15 per store), expanding to 75 users.
* Existing devices: 3 POS terminals per store, 10 desktop computers, 3 wireless routers, 1 printer per store.
* Coverage requirements: Each store needs coverage for 200 square metres.
* Number of rooms: 3 rooms per store (retail, storage, office).
* Access points: 2 access points per store.
* Uses: Messaging, emails, web browsing, basic file sharing.

**Traffic demands:**

Current:

* Data traffic: Primarily generated by POS systems, inventory management, and internal communications (emails, messaging).
* Peak times: During business hours, especially weekends and public holidays when customer traffic is high.
* Bandwidth usage: Moderate, primarily supporting sales transactions, inventory updates, and basic file sharing between stores.
* Applications: Cloud-based inventory systems, web browsing for product look-up, internal email, and occasional video calls between store managers.

Estimated data usage:

* Per Store: 50–100 GB per month
* Overall: 150–300 GB per month for all existing stores

Future traffic demands:

* Expansion: With 2 additional stores, the overall data usage is expected to increase by 30-40%.
* Increased cloud usage: More reliance on cloud services for real-time inventory management and customer data processing.
* POS system upgrades: Potentially higher data traffic due to the implementation of more advanced POS features, like integrated customer loyalty programs.
* Additional services: Introduction of in-store digital marketing (e.g., video streaming for promotions), increasing bandwidth requirements.

Projected Data Usage:

* Per Store: 75–125 GB per month
* Overall: 375–625 GB per month for all stores after expansion

**Site access arrangements:**

* Existing stores: Access during non-business hours (evenings or weekends) to minimise disruption to operations.
* New stores: Access during the fit-out phase, before the store is open to the public.
* Key personnel: Store managers and IT staff should be available for consultation during installation.

**Security arrangements**

**Physical Security:**

* Secure site access by using keycards or PIN codes for authorised personnel only. Contractors and IT staff will have limited access during installation times, with access restricted to specific areas (e.g., server rooms).
* All store entrances, exits, and key areas (e.g., POS stations, storage rooms) are monitored by security cameras, especially during after-hours installations.
* Existing alarm systems to alert store managers or security personnel in case of unauthorised access during network installations.

**Network Security:**

* During installation, contractors must isolate the store’s network from the main network to prevent unauthorised access or data breaches. Once installation is complete, test and securely reintegrate the store's network.
* Ensure that any data migrations or system updates conducted during site visits are encrypted and backed up to prevent data loss or unauthorised access.

**Personnel Security:**

* Background checks are required on any third-party contractors or IT personnel involved in the installation process.
* All external personnel to sign NDAs to protect the company’s confidential data and network design details.

**Simulation 2: Urban Accountancy Solutions**

Urban Accountancy Solutions is a growing accounting firm moving its main office to a larger space within the same city. The new office will house 30 employees, including accountants, administrative staff, and managers.

**Overall objective:** The firm needs an ICT network architecture that supports secure data handling, basic video conferencing, and email communication.

**Business problem:**

The company handles sensitive financial data, including tax returns and client financial statements. Currently, data transmission between the office and remote workers is not fully secured, posing risks of data breaches and non-compliance with data protection regulations.

**Business opportunity:**

A robust VPN and enhanced encryption could ensure secure communication between the office, remote workers, and clients. This not only addresses current security concerns but also positions the firm as a trustworthy and compliant provider of financial services.

**Budget:** $40,000–$60,000

**Timeline:** 6 weeks

**Details and specifications**

* Existing network type: small office LAN.
* Number of users: 20 existing users, expanding to 30 users.
* Existing devices: 20 desktop computers, 2 printers, 1 video conferencing system, 2 network switches, 1 router, and 1 firewall.
* Coverage requirements: 500 square metres.
* Number of rooms: 10 rooms (5 offices, 2 meeting rooms, 3 general areas).
* Access points: 4 access points needed.
* Uses: Messaging, emails, video calls, web browsing, file sharing.

**Traffic demands:**

Current:

* Data Traffic: Generated by secure file sharing, emails, web browsing, and video conferencing.
* Peak Times: During normal business hours (Monday to Friday), especially during tax season or client deadlines.
* Bandwidth Usage: Moderate to high due to frequent file transfers of large financial documents and regular video conferencing.
* Applications: Email, secure cloud storage, financial software, web-based research, and internal messaging.

Estimated Data Usage:

* Per User: 100–150 GB per month
* Overall: 2,000–3,000 GB per month for all users

Future Traffic Demands:

* Expansion: The move to a larger office with more staff will increase data usage proportionately.
* Increased Remote Work: Growing reliance on remote work capabilities could lead to higher VPN and cloud storage traffic.
* Video Conferencing: More frequent use of video calls and conferencing due to client interactions and internal meetings.
* Advanced Security Measures: Implementation of more robust security protocols (e.g., data encryption, intrusion detection) may slightly increase overhead but is necessary to handle sensitive financial data.

Projected Data Usage:

* Per User: 125–175 GB per month
* Overall: 3,750–5,250 GB per month for all users after expansion

**Site access arrangements**

* Current office: Access during after-hours or weekends for minimal disruption.
* New office: Access during the fit-out phase, before employees move in.
* Key personnel: IT manager and office manager should be available to coordinate the move.

**Security arrangements**

**Physical Security:**

* Biometric access controls (e.g., fingerprint or facial recognition) are used for sensitive areas like the server room. Physical access is limited to authorised personnel only, such as IT staff and senior management.
* All visitors, including contractors, must sign in and be issued temporary access cards with limited permissions.
* Security cameras and alarm systems are operational in key areas, such as the data centre, IT equipment rooms, and office entrances.

**Network Security:**

* The network should be segmented during the transition phase to isolate critical systems from the rest of the network. This limits potential security risks while the new network is being set up.
* Ensure that all data transfers during the move are encrypted and use secure channels like VPNs for remote access during the transition period.
* Conduct a security audit before and after the installation to identify vulnerabilities and ensure compliance with data protection standards.

**Personnel Security:**

* Strict access policies are enforced where only authorised IT staff can access the server room and network hardware during the installation process.
* Two-Factor Authentication (2FA) applies for all IT personnel accessing sensitive systems, ensuring an additional layer of security during installation and setup.