NCIA NETWORK REFERENCE

Scenario 1: "Glass House" — Supporting Material

FOR TRAINING USE ONLY

NCIA NETWORK VLAN MAP

North Coast International Airport segments its network into multiple Virtual Local Area Networks (VLANs) to separate different types of traffic. Each VLAN is a logically isolated network — devices on one VLAN should not be able to see or talk to devices on another VLAN unless the core switch and firewall explicitly allow it.

VLAN	Name	Subnet	Purpose	Key Devices
10	Server VLAN	10.1.10.0/24	Production servers — payment gateway, AODB, FIDS server, email server, file server.	Payment Gateway (10.1.10.15) AODB Server (10.1.10.20) FIDS Server (10.1.10.25) Domain Controller (10.1.10.5)
20	Admin / Corporate VLAN	10.1.20.0/24	Airport admin workstations, HR, finance, executive offices, IT staff workstations.	IT Manager Workstation (10.1.20.10) HR Workstations (10.1.20.50-60) Ops Director PC (10.1.20.30)
30	Security Camera VLAN	10.1.30.0/24	IP cameras, NVR (Network Video Recorder), PACS interface.	NVR (10.1.30.5) 47 IP Cameras PACS Controller (10.1.30.10)
40	Retail / Vendor VLAN	10.1.40.0/24	All tenant POS terminals, vendor back-office PCs, concession kiosks.	SkyLounge POS (10.1.40.101) Duty-Free #1 POS (10.1.40.110) Duty-Free #2 POS (10.1.40.115) Food Court POS cluster (10.1.40.120-130)
50	Passenger Wi-Fi VLAN	10.1.50.0/24	Public-facing Wi-Fi for passengers and visitors. Should be fully isolated from internal VLANs.	Wi-Fi Controllers Captive Portal Server
60	Baggage / OT VLAN	10.1.60.0/24	Baggage handling system, operational technology, airside systems.	BHS Controller (10.1.60.5) Gate Management System
99	Management VLAN	10.1.99.0/24	Switch management interfaces, firewall admin, out-of-band management.	Core Switch Mgmt (10.1.99.1) Firewall Mgmt (10.1.99.2)

KEY PERSONNEL — IT DEPARTMENT

Name	Title	Access Level	Notes
Jordan Kelley	IT Manager	Domain Admin, Firewall Admin, Physical key to all server rooms, PACS override	10-year employee. Has root/admin access to every system at NCIA. Sole holder of firewall admin credentials.
Priya Deshmukh	Network Technician	Read-only on switches, no firewall access	3-year employee. Handles day-to-day cabling, Wi-Fi issues, helpdesk tickets.
Marcus Chen	Systems Administrator	Server admin (VLAN 10 only), no firewall access	5-year employee. Manages servers, backups, patches. Does not have physical key to secondary server closet.

PHYSICAL LAYOUT — SERVER ROOMS

Primary Server Room (Room 142, Admin Corridor): Houses the core switch, firewall, payment gateway server, AODB server, FIDS server, domain controller, and NVR. Access controlled by PACS badge + PIN. Door alarm logs to the AOC. Climate controlled at 68°F. Jordan Kelley, Marcus Chen, and the Ops Director hold badge access.

Secondary Server Closet (Room 217, Maintenance Hallway near Concourse B): Houses a secondary network switch, a legacy backup server (scheduled for decommission 18 months ago — still powered on), a patch panel for Concourse B retail tenants, and the Wi-Fi controller for Concourse B. Access is controlled by a physical key lock — not on the PACS system. Jordan Kelley holds the only key. No climate monitoring. No security camera covering this door.

Note: The gap in physical security at Room 217 is intentional for this exercise. It reflects a common real-world weakness at airports — secondary IT closets that fall outside the access-control perimeter.