**📡 Enterprise-Level Network Implementation Report – Tim Hortons Branches**

**Prepared by: Prince Singh**

**Role: Network Engineer**

**Tools Used: Cisco Packet Tracer, CLI, GUI**

**Technologies: VLAN, DHCP, Trunking, OSPF, SSH, Wi-Fi (WRT300N), Sub-interfaces, Inter-VLAN Routing**

**🔷 Overview**

This project simulates a realistic **multi-branch enterprise network** architecture for Tim Hortons, consisting of the following sites:

* **Wolverhampton (Head Office)**
* **Birmingham Branch**
* **London Branch**
* **Manchester Branch**

Each branch includes staff and guest wireless networks, VLAN separation, printers, PCs, and routers connected with head office via OSPF and secured with SSH remote access.

**🗺️ Network Topology Summary**

* **Core**: Head Office (Wolverhampton) Router connects to all branches.
* **Interconnectivity**: Site-to-site links use /30 subnets.
* **Branch Components**: Switches, WRT300N for Wi-Fi, PCs, Printers.
* **VLANs**:
  + **Staff Wi-Fi VLAN**: Branch-specific VLAN (e.g., VLAN 10, 30, 50, 70)
  + **Guest Wi-Fi VLAN**: Branch-specific VLAN (e.g., VLAN 20, 40, 60)

**🛠️ Step-by-Step Configuration**

**1️⃣ VLAN & Switch Configuration (Per Branch)**

* Created VLANs:
  + Staff Wi-Fi (e.g., VLAN 10, 30, 50, 70)
  + Guest Wi-Fi (e.g., VLAN 20, 40, 60)
* Assigned ports to VLANs.
* Configured trunk port to the router.

**Example (Birmingham):**

I have created **two VLANs** on the switch:

* **VLAN 10** → Tim\_Staff\_Wifi
* **VLAN 20** → Tim\_Guest\_Wifi

You assigned ports accordingly:

**🔹 VLAN 10 (Staff):**

A screenshot of a computer

AI-generated content may be incorrect.

🔗 3. Set the Trunk Port (Gigabit0/1)

This port connects the switch to the Birmingham router, and it must carry traffic for both VLANs.

A screenshot of a computer

AI-generated content may be incorrect.

**4. Subinterface Configuration on Router**

You configured **subinterfaces** on the router to act as **gateways for each VLAN**:

bash

A screenshot of a computer

AI-generated content may be incorrect.

These IPs act as **default gateways** for all devices in their respective VLANs.

**2️⃣ Router-on-a-Stick & DHCP Configuration**

* Sub-interfaces for each VLAN on the router.
* Configured encapsulation dot1q for each VLAN.
* Set up **DHCP pools** to auto-assign IPs.

**Example (London):**

We enabled **automatic IP assignment** by creating DHCP pools:

A computer screen shot of a computer program

AI-generated content may be incorrect.This means:

* Devices in VLAN 10 will automatically get IPs from 192.168.10.11 - 192.168.10.254
* Devices in VLAN 20 will get IPs from 192.168.20.11 - 192.168.20.254
* Gateways are excluded from the pool

**Testing & Verification**

You verified the setup by:

* Going to **each PC's desktop → IP Configuration → DHCP**
* Checking the assigned IP address, subnet, and gateway

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

* Running ping tests to:
  + Ping the router (192.168.10.1 / 192.168.20.1)
  + Ping other devices in the same or different VLAN
  + Test if network is working (all succeeded)

A computer screen shot of a black screen

AI-generated content may be incorrect.

| **Component** | **Purpose** |
| --- | --- |
| **VLANs** | Separate network for Staff and Guest traffic |
| **DHCP** | Auto-assign IPs, reduce manual config |
| **Trunk Port** | Carry multiple VLANs over 1 port to router |
| **Router Subinterfaces** | Gateways for VLANs and inter-VLAN routing |
| **Ping Tests** | Confirmed network functionality and device reachability |

**3️⃣ Wi-Fi Configuration (WRT300N)**

* Used **WRT300N routers** to create:
  + **Staff SSID** (e.g., Tim\_Staff\_London)
  + **Guest SSID** (e.g., Tim\_Guest\_London)
* Disabled DHCP on WRT300N.
* Connected WRT300N to respective switch ports (VLAN-based).

**Staff & Guest Devices** obtained IP addresses dynamically from branch DHCP.

**🧱 Step-by-Step Breakdown**

1. **Used Devices**

* **2 WRT300N Wireless Routers (Access Points)**:
  + One for **Staff**
  + One for **Guests**

WRT300N in Packet Tracer supports only **one SSID per device**, so we use **two separate WRT300Ns**.

1. **Physical Cable Connections**

You made **wired connections** between the WRT300Ns and the switch:

| **Switch Port** | **Device** | **Purpose** | **VLAN** |
| --- | --- | --- | --- |
| Fa0/1 | WRT300N (Staff Wi-Fi) | Staff Access | 10 |
| Fa0/8 | WRT300N (Guest Wi-Fi) | Guest Access | 20 |

These ports were **set to access mode** and placed into the **correct VLANs**, so traffic from the WRT300Ns gets tagged properly.

1. **Switch VLAN Assignment**

interface Fa0/1

switchport mode access

switchport access vlan 10

interface Fa0/8

switchport mode access

switchport access vlan 20

This means:

* Devices connecting to **Staff Wi-Fi** are in VLAN 10
* Devices connecting to **Guest Wi-Fi** are in VLAN 20

1. **Wireless Router (WRT300N) Configuration**

You configured the WRT300N **via GUI**:

**👨‍💼 Staff Wi-Fi (Router #1)**

* **SSID**: Tim\_Staff\_Wifi
* **DHCP**: **Disabled** (to avoid conflicts—we’re using the **router DHCP**)
* **Gateway/DNS**: Point to **router IP**: 192.168.10.1

**A screenshot of a computer

AI-generated content may be incorrect.**

**🎟️ Guest Wi-Fi (Router #2)**

* **SSID**: Tim\_Guest\_Wifi
* **DHCP**: **Disabled**
* **Gateway/DNS**: 192.168.20.1

You accessed the router GUI by clicking the WRT300N → **GUI tab** → Basic/Setup Settings.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Laptop & Smartphone Connection**

You connected wireless devices:

* **Laptop** → connected to **Tim\_Staff\_Wifi**

A screenshot of a computer

AI-generated content may be incorrect.

* **Smartphone** → connected to **Tim\_Guest\_Wifi**

A screenshot of a computer

AI-generated content may be incorrect.

Then you:

* Opened their **Desktop tab**
* Clicked **IP Configuration**
* Ensured **DHCP** was selected

They received:

* Staff laptop: IP from **192.168.10.0/24** range
* Guest phone: IP from **192.168.20.0/24** range

1. **Testing Wi-Fi**

You tested the connection by:

* Opening **Command Prompt** on the **laptop**
* Running:

ping 192.168.10.1

And similarly for:

ping 8.8.8.8

You could also test the **web browser**:

* Go to the **Desktop tab**
* Open **Web Browser**
* Type a valid IP or simulate local web server if configured

**🧠 Why This Design Works**

| **Wi-Fi** | **Connected Device** | **VLAN** | **DHCP Source** | **Gateway** | **IP Range** |
| --- | --- | --- | --- | --- | --- |
| Staff | Laptop | 10 | Birmingham Router | 192.168.10.1 | 192.168.10.11–254 |
| Guest | Smartphone | 20 | Birmingham Router | 192.168.20.1 | 192.168.20.11–254 |
|  |  |  |  |  |  |

✅ **Benefits**:

* **Isolation**: Staff and Guest traffic is separated by VLAN
* **Security**: Guest devices cannot access Staff devices or printers
* **Automatic Configuration**: DHCP assigns IPs to wireless devices automatically
* **Scalability**: Easy to add more devices without manual IP setup

A screen shot of a computer

AI-generated content may be incorrect.

**4️⃣ Routing – OSPF Configuration**

Enabled **OSPF** on all routers to allow dynamic route exchange and inter-branch communication.

**Example (Head Office):**

router ospf 1

network 192.168.70.0 0.0.0.255 area 0

network 10.10.10.0 0.0.0.15 area 0

network 10.10.10.4 0.0.0.3 area 0

network 10.10.10.8 0.0.0.3 area 0

Branch routers were similarly configured to advertise internal VLAN networks and /30 point-to-point links.

**🧱 Network Topology Overview:**

| **Branch** | **VLAN** | **Subnet** | **Link to HO Subnet** |
| --- | --- | --- | --- |
| Wolverhampton | 70 | 192.168.70.0/24 | — |
| Manchester | 50 | 192.168.50.0/24 | 10.10.10.0/30 |
| Birmingham | 10 | 192.168.10.0/24 | 10.10.10.4/30 |
| London | 30 | 192.168.30.0/24 | 10.10.10.8/30 |

**⚙️ Configuration Steps (Summary):**

**1. On Wolverhampton Router:**

Enabled OSPF and advertised:

* Internal staff network (192.168.70.0/24)
* All branch point-to-point links:
  + 10.10.10.0/30 (Manchester)
  + 10.10.10.4/30 (Birmingham)
  + 10.10.10.8/30 (London)

A black text on a white background

AI-generated content may be incorrect.

A close-up of a number

AI-generated content may be incorrect.

A screenshot of a computer code

AI-generated content may be incorrect.

A close-up of a number

AI-generated content may be incorrect.

router ospf 1

network 192.168.70.0 0.0.0.255 area 0

network 10.10.10.0 0.0.0.3 area 0

network 10.10.10.4 0.0.0.3 area 0

network 10.10.10.8 0.0.0.3 area 0

**2. On Each Branch Router:**

Enabled OSPF and advertised:

* Their internal VLAN network (e.g., 192.168.50.0/24 for Manchester)
* Their link to the head office (e.g., 10.10.10.0/30 for Manchester)

**Example (Manchester)**:

router ospf 1

network 192.168.50.0 0.0.0.255 area 0

network 10.10.10.0 0.0.0.3 area 0

Same logic was applied to **Birmingham** and **London** with their respective subnets.

A screenshot of a computer program

AI-generated content may be incorrect.

**🔍 Verification & Testing:**

From the **Admin PC at Wolverhampton** (IP: 192.168.70.X), the following tests were performed:

ping 192.168.10.2 # Birmingham PC

ping 192.168.30.2 # London PC

ping 192.168.50.2 # Manchester PC

✅ All ping tests were successful, confirming full connectivity.

A screenshot of a computer

AI-generated content may be incorrect.

**🧠 Explanation:**

**Why OSPF?**

* OSPF is a link-state dynamic routing protocol.
* It automatically discovers and shares route information.
* Avoids the manual effort of static route configuration.
* Automatically updates routing tables if links go down or topology changes.

**Benefits Achieved**:

* The **Admin PC** at the head office can now fully manage and access all devices across all branches.
* Network is now **scalable** and **self-updating** in terms of routing.
* This setup also simplifies network management and troubleshooting.

**5️⃣ SSH Secure Remote Access**

* Set hostnames and domain.
* Generated crypto keys.
* Created a user with privilege 15.
* Enabled VTY lines for SSH only.

**Example:**

hostname London\_Router

ip domain-name timhortons.local

crypto key generate rsa

username admin privilege 15 secret TimLondon@123

line vty 0 4

transport input ssh

login local

**Admin PC (192.168.70.12)** from Wolverhampton uses SSH to access all routers remotely.

A screenshot of a computer code

AI-generated content may be incorrect.

A white screen with black text

AI-generated content may be incorrect.

A screenshot of a computer code

AI-generated content may be incorrect.

Great! Here's your **final report** summarizing the **SSH configuration and access control** implemented across all routers in your network. This can be used for documentation, audits, or presentations.

**🧾 Final SSH Security Configuration Report**

**📍 Project Name: Secure Centralized Router Access via SSH**

**🏢 Network Head Office: Wolverhampton**

**🧑‍💻 Admin PC IP: 192.168.70.12**

**🔒 Purpose: Restrict router access to only the Admin PC for secure and centralized management**

**🔐 Objective**

To ensure that only the **Admin PC in Wolverhampton Head Office** is allowed to remotely manage the network routers via **SSH**, while blocking SSH access from all other devices (including staff, HR, guest Wi-Fi, and public PCs).

**📡 Devices Covered**

| **Branch** | **Router IP** | **Allowed via SSH from Admin PC** |
| --- | --- | --- |
| Birmingham | 192.168.10.1 | ✅ Yes |
| London | 192.168.30.1 | ✅ Yes |
| Manchester | 192.168.50.1 | ✅ Yes |
| Wolverhampton (HO) | 192.168.70.1 | ✅ Optional (configured if needed) |

**⚙️ SSH Access Control Configuration (on each router)**

**📌 Commands Applied:**

enable

configure terminal

access-list 10 permit 192.168.70.12

line vty 0 4

access-class 10 in

end

write memory

* access-list 10 permit 192.168.70.12: Allows SSH from Admin PC only
* access-class 10 in: Applies this ACL to VTY lines (SSH sessions)
* line vty 0 4: Refers to SSH virtual terminal lines
* write memory: Saves the configuration

**🧪 Testing Performed**

| **Test Scenario** | **Result** |
| --- | --- |
| SSH from Admin PC to Birmingham | ✅ Success |
| SSH from Admin PC to London | ✅ Success |
| SSH from Admin PC to Manchester | ✅ Success |
| SSH from any other PC (Staff/HR) | ❌ Denied (Connection Closed) |
| SSH from Guest Wi-Fi Smartphone | ❌ Denied |

**🛡️ Benefits of This Configuration**

| **Advantage** | **Description** |
| --- | --- |
| **Security** | Blocks all unauthorized access to critical router configs |
| **Centralized Control** | Only authorized Admin PC can make changes |
| **Compliance** | Aligns with security policies (least privilege principle) |
| **Accountability** | Easier to track changes and logins from one secured device |

**🎯** Purpose:

This says:

“Only allow SSH access if it comes from the IP 192.168.70.12 — the Admin PC.”

🛡️ Result:

Admin PC: Can SSH into any router ✔️

All Other Devices (staff, HR, guests): Blocked ❌

A computer screen shot of a computer program

AI-generated content may be incorrect.

**6️⃣ Security Segmentation**

* Ensured **Guest VLANs were isolated** using VLAN configuration.
* Only routers with routing capability connected VLANs.
* Tested ping to ensure guest devices **could not reach** staff VLANs.

**🧪 Testing & Validation**

✔️ DHCP verified: All devices received dynamic IP addresses  
✔️ Ping test passed: Inter-VLAN & inter-branch communication functional  
✔️ SSH tested: Admin PC could securely manage routers  
✔️ Isolation verified: Guest network couldn't access Staff devices

**💼 Skills Demonstrated**

* Enterprise-level VLAN & subnet design
* Secure network segmentation
* OSPF configuration for multi-branch routing
* DHCP deployment with multiple VLANs
* SSH for secure router access
* Wi-Fi segmentation & device integration
* Troubleshooting and logical testing

**🎯 Final Outcome**

The fully functional simulated network reflects a real-world **enterprise deployment**. The design supports:

* Secure, scalable Wi-Fi and wired access
* Remote administration via SSH
* Centralized control from the Head Office
* Efficient dynamic IP management
* Isolation of guest traffic