Network Design Report on Intercom XP (Communication Organisation)

Date of Completion: 1st January 2024

Table of Contents

1. Introduction.....2

1.1. Overview of Intercom XP & Network Infrastructure.....2

1.2. Expected Results of Proposed Network Design.....3

2. Networking Design & Configuration.....3

2.1. Architecture & Justification of the Network Configuration.....4

3. Naming Conventions for Network Devices.....5

4. IP Addressing Design Scheme.....6

5. VLANS & Logical Partitioning.....7

6. Network Troubleshooting & Maintenance Strategy.....7

6.1. Strategies & Potential Issues.....5

6.2. Management & Growth.....6

7. Conclusion.....7

8. Reference List.....7

Introduction

This report highlights and evaluates the overall World Area Network configuration for a communication company, operating in the United Kingdom and Switzerland. The network embeds Cisco's hierarchical network design model which involves applying three layers: Access, Distribution and Core (Cisco Press, 2014). Reliable security measures are implemented to deter and engage against external and internal threats by the support of several technical and non-technical features and protocols. General networking practices and optional components are mentioned to be practically embedded to complete specific requirements for a successful configurated network.

1.1. Overview of Intercom XP & Network Infrastructure

Intercom XP is an international communication company based in the United Kingdom with operations within Switzerland with a total employee count of 2000. The main headquarter is stationed in the UK with a number of 1200 staff members while the Swiss site holds 800 members. Each headquarter consists of three departments, containing their networking team which are responsible for the overall construction, operations and maintenance of their Local Area Network configuration:

- **Network Design & Operations** -> responsible for the design and maintenance of the network, including implementing security and handle troubleshooting.

- **Technical Support** -> provides installation of network hardware, customer support queries and collaborates with network engineers to configure.

- **Training** -> offers awareness general networking security, technical training to new employees and responsible for network recovery.

This network configuration operates between two headquarters within different countries, classifying it as a WAN. Various hardware and networking components for physical and logical connections within each site are expected to be enabled including routers and switches for connectivity with devices and external networks while multitude of specific requirements were addressed to consider cost, security, performance, continuous scalability and redundancy. It is vital to select and efficiently implement specific networking practices with specialized tools to their potential for high-quality performance in terms of communication and security while minimizing costs and enable chances for scalability for the network to develop as hardware devices become obsolete (Stallings, 2014; Tanenbaum & Wetherall, 2011). Secure communication links are expected using physical and logical deterrents along with

segmentation, access control, authentication techniques and monitoring tools. Subnetting, VLANS and firewalls are key security components found within each headquarters' network (Kaeo, 2004). Finally, it is important to create secondary network pathways to retain available consistent connections between hardware during specific network failure therefore the configuration includes redundancy. Cisco Systems specializes in networking hardware, software and telecommunications, sharing technical recommendations on general networking. For example, for optimal performance, a fast Internet connection with a standard bandwidth of 512kbps or more should be used for constant data handling applications (Cisco, 2023). A high-capacity bandwidth when connecting to cloud services through the Internet would be required.

1.2. Expected Results of Proposed Network Design

At the end of initiating the startup of the configuration, the discussed factors mentioned prior must be fulfilled on a frequent level. Both headquarters must have reliable connection and rapid communication with each another with minimal issues adhering to rules and regulations on security. It should be expected to flexibly allow scalability and redundancy, embedding core, distribution and access layers (Cisco Press, 2014).

2. ***Networking Design & Configuration***

Figure 1 – physical mode (intercity view) on Cisco Packet Tracer

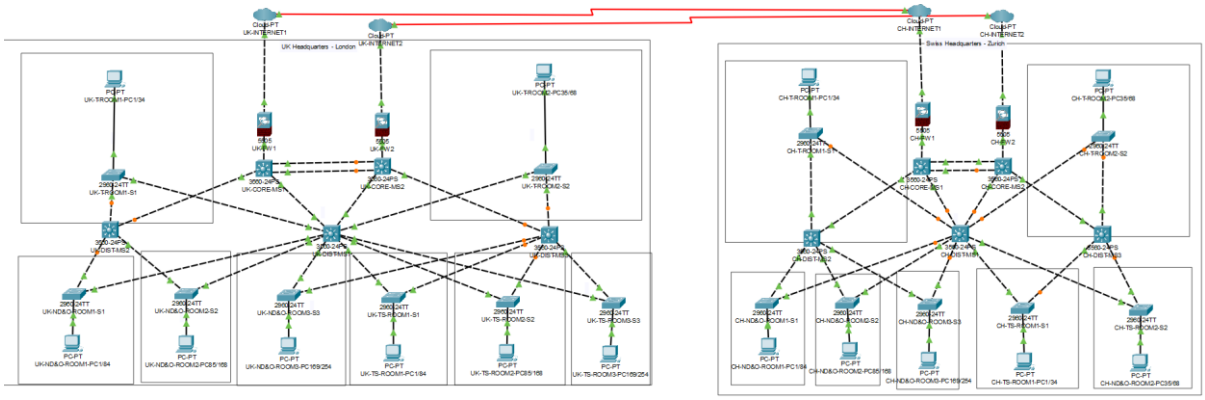

Figure 2 – overall Intercom XP network configuration on Cisco Packet Tracer

2.1. Architecture & Justification of the Network Configuration

Figure 1 and 2 represent both Intercom XP headquarters physically and logically. All headquarters possess all three departments with each staff count:

***UK HEADQUARTERS*: 1200 EMPLOYEES | SWISS *HEADQUARTERS*: 800 EMPLOYEES**

- 500 staff (UK), 200 staff (Switzerland) -> Network Design & Operations
- 500 staff (UK), 500 staff (Switzerland) -> Technical Support
- 200 staff (UK), 100 staff (Switzerland) -> Training

Within the capital headquarters (UK), ND&O and TS hold three rooms possessing around 84 PCs each for 2 users to share a single PC. On the other hand, the Training department has two rooms with an estimate of 34 PCs for 2 users each. In the Swiss site hand, TS owns two rooms with 34 PCs for 2 users each similar to the Training rooms. All rooms may be permitted to store additional end devices such as printers and servers which strictly depends on IP address allocation (discussed in Chapter 4), connecting all devices to a Layer 2 switch in their own LANs in the Access Layer.

It is highlighted and managed for general end device connectivity with distribution devices in order to receive and transfer network traffic throughout the entire headquarter network. Usually, basic networking practices such as segmentation and security measures are implemented in this layer (Cisco Press, 2014). These practices offer better manageability of the network and reduces the chances of security breaches due to isolated network traffic to specific departments, rooms or headquarters. VLANS and subnetting are key examples of network segmentation within the Local Area Network of each headquarter to segment the departments and rooms logically, allocating devices with private classless IP addresses. These private IP addresses are crucial due to reliable security against external parties accessing the associated host (Kaeo, 2004). Additionally, unused ports on all devices should be switched off to

prevent unauthorized access combined with MAC address filtering as access control. Apart from involving basic security using isolation, it is essential to prevent a critical single point in failure in the access layer as failure to do so leads to severe problems with accessing significant data for staff members in real-time therefore redundancy is a major factor to cover. For redundancy on this layer, Layer 2 switches in all rooms are automatically connected to the main Distribution Multi-Layer switch and a secondary Distribution Multi-Layer Switch. The secondary switch acts like a backup routing unit in the event the main Distribution Multi-Layer switch is down.

For routing between the Access and the Core Layer, we have a Distribution layer which manages three Layer 3 Multi-Layer switches responsible for connectivity and routing (Cisco Press, 2014). Previously mentioned, a main multi-layer switch routes the network traffic to both Core Layer switches however the secondary Distribution Multi-Layer switches commit these functionalities as well to enable load balancing and fault tolerance for the networks due to little dependency for the main distribution while maintaining an operational network. As a result, overall network performance with traffic transfer speeds improves, easier monitoring and troubleshooting by decomposing the network and a potential for scalability is unlocked as additional multi-layer switches or routers can be implemented. Static routing is configured for traffic flow control as it grants security and predictability for troubleshooting with access control lists (Kaeo, 2004). It is at this layer which the VLANS for the departments are configured and managed using inter-VLAN routing on the distribution switches.

Finally, the Core Layer will support high-capacity data packet traffic routing to and from external networks and services. A set-up of two Layer 3 multi-layer switches with a high-capacity in bandwidth and a large switching capacity for data exchange is the standard (Cisco Press, 2014). An EtherChannel was configured for additional bandwidth and backs up redundancy, especially for this layer as it forwards vigorous amounts of data traffic from the distribution layer so downtime would be critical. To add more principles, dynamic routing is included instead of static routing as the core switches interacts with external networks with public IP addresses which requires automatic updating to access the Internet/Cloud Provider services. Physical firewalls are implemented before data traffic transfers to external networks to filter and block unauthorized traffic, reducing the chances of cyberattacks from external parties.

3. ***Naming Conventions for Network Devices***

All devices follow the naming scheme, providing a simple summary on the location, functionality and uniqueness of the device within the LAN and WAN configuration:

“[Country] - [Department] - [Room Number] - [Layer] - [Device Type & ID]”

Country -> refers to the country of the headquarter where the device is located. The abbreviation for the country is labelled (Canada, CA).

Department -> the abbreviation of the department for end devices and layer 2 switches within the rooms (Technical Support, TS).

Room Number -> the room number where the device is located (if applicable).

Layer -> the hierarchical modelling layer of the device (Distribution, DIST)

Device Type & ID -> the unique identifier for the device (Switch 1, SW1)

There are some exceptions such as the Distribution and Core devices with no department and room tags as they remain disassociated logically but physically it would differ. They would most likely be kept within another room or floor.

4. ***IP Addressing Design Scheme***

IP addresses are the key aspect of networking which allows end-devices and interfaces to access resources using the address as a label. Intercom XP’s network configuration contains public and private IP address for specific purposes. They are configured within subnets and VLANS on specific interfaces. Two IP address tables for each LAN network of the headquarters have been produced to highlight the devices, interfaces, subnet masks, IP addresses ranges, default gateway and VLANS for documentation purposes.

UK Headquarters

Device	Interface	IP Address	Subnet Mask	Default Gateway
UK-DIST-MS1	VLAN 30 VLAN 60 VLAN 90	192.168.30.1/24 192.168.60.1/24 172.16.90.1/25	255.255.255.0 255.255.255.0 255.255.255.128	N/A
UK-DIST-MS2	VLAN 30 VLAN 60 VLAN 90	192.168.30.2/24 192.168.60.2/24 172.16.90.2/25	255.255.255.0 255.255.255.0 255.255.255.128	N/A
UK-DIST-MS3	VLAN 30 VLAN 60 VLAN 90	192.168.30.3/24 192.168.60.3/24 172.16.90.3/25	255.255.255.0 255.255.255.0 255.255.255.128	N/A

UK-CORE-MS1	VLAN 30 VLAN 60 VLAN 90	10.0.30.1/16 10.0.60.1/16 10.0.90.1/16	255.255.0.0 255.255.0.0 255.255.0.0	N/A
UK-CORE-MS2	VLAN 30 VLAN 60 VLAN 90	10.0.30.2/16 10.0.60.2/16 10.0.90.2/16	255.255.0.0 255.255.0.0 255.255.0.0	N/A
UK-FW1	Et0/1 Et0/0	84.0.100.1 10.10.0.5/32	N/A	10.10.0.1
UK-FW2	Et0/1 Et0/0	198.0.100.1 10.10.0.10/32	N/A	10.10.0.1

Swiss Headquarters

Device	Interface	IP Address	Subnet Mask	Default Gateway
CH-DIST-MS1	VLAN 30 VLAN 60 VLAN 90	192.168.30.1/24 192.168.60.1/24 172.16.90.1/25	255.255.255.0 255.255.255.0 255.255.255.128	N/A
CH-DIST-MS2	VLAN 30 VLAN 60 VLAN 90	192.168.30.2/24 192.168.60.2/24 172.16.90.2/25	255.255.255.0 255.255.255.0 255.255.255.128	N/A
CH-DIST-MS3	VLAN 30 VLAN 60 VLAN 90	192.168.30.3/24 192.168.60.3/24 172.16.90.3/25	255.255.255.0 255.255.255.0 255.255.255.128	N/A
CH-CORE-MS1	VLAN 30 VLAN 60 VLAN 90	10.0.30.1/16 10.0.60.1/16 10.0.90.1/16	255.255.0.0 255.255.0.0 255.255.0.0	N/A
CH-CORE-MS2	VLAN 30 VLAN 60 VLAN 90	10.0.30.2/16 10.0.60.2/16 10.0.90.2/16	255.255.0.0 255.255.0.0 255.255.0.0	N/A
CH-FW1	Et0/1 Et0/0	84.0.100.1 10.10.0.5/32	N/A	10.10.0.1
CH-FW2	Et0/1 Et0/0	198.0.100.1 10.10.0.10/32	N/A	10.10.0.1

5. ***VLANS & Logical Partitioning***

The following VLANS for each department:

Network Design & Operations for VLAN 30
Technical Support for VLAN 60
Training for VLAN 90

The table below highlights the logical partitioning of the two LAN configurations.

UK Headquarters

Department	Subnet Prefix	Subnet Mask	Usable IP Address Ranges	Default Gateway	VLAN ID	VLAN Interfaces	Rooms /Total PC Count
Network Design & Operations	192.168.30.0/24	255.255.255.0	Room 1 -> 192.168.30.1 to 192.168.30.84 Room 2 -> 192.168.30.85 to 192.168.30.168 Room 3 -> 192.168.30.169 to 192.168.30.254	192.168.30.1	30	192.168.30.1	3 /252
Technical Support	192.168.60.0/24	255.255.255.128	Room 1 -> 192.168.60.1 to	192.168.60.1	60	192.168.60.1	3 /252

			192.168.60.84 Room 2 -> 192.168.60.85 to 192.168.60.168 Room 3 -> 192.168.60.169 to 192.168.60.254				
Training	172.16.90.0/25	255.255.255.0	Room 1 -> 172.16.90.1 to 192.168.30.35 Room 2 -> 172.16.90.36 to 172.16.90.126	172.16.90.1	90	172.16.90.1	2 /68

Swiss Headquarters

Department	Subnet Prefix	Subnet Mask	Usable IP Address Ranges	Default Gateway	VLAN ID	VLAN Interfaces	Rooms /Total PC Count
Network Design & Operations	192.168.30.0/24	255.255.255.0	Room 1 -> 192.168.30.1 to	192.168.30.1	30	192.168.30.1	3 /252

			192.168 .30.84 Room 2 -> 192.168 .30.85 to 192.168 .30.168 Room 3 -> 192.168 .30.169 to 192.168 .30.254				
Technical Support	192.168. 60.0/24	255.25 5.255.0 128	Room 1 -> 172.16. 60.1 to 172.16. 60.84 Room 2 -> 172.16. 60.85 to 172.16. 60.168	172.16.6 0.1	60	172.16.60. 1	2 /68
Training	172.16.9 0.0/25	255.25 5.128.0	Room 1 -> 172.16. 90.1 to 192.168 .30.35 Room 2 -> 172.16. 90.36 to 172.16. 90.126	172.16.9 0.1	90	172.16.90. 1	2 /68

6. ***Network Troubleshooting & Maintenance Strategy***

6.1. Strategies & Potential Issues

Occurrences in issues will always exist for the network in the future like slow or lost connections to certain devices or services, security breaches, etc therefore several troubleshooting methods may be included to mitigate and resolve these potential issues. Each Network Design & Operations team in their respective departments should properly document their local network configuration while collaborating to maintain updated versions of the entirety of the network configuration between the two headquarters. This means recording and monitoring down all devices, IP addresses, VLANS and any other relevant networking aspects to identify growing problems early.

Checks will need to be put in place from physical hardware to logical features to make sure everything is operational. Generally, when networks are troubleshooted the OSI model is considered to incrementally check each layer of the model to find issues.

Additionally, certain packet tracer applications such as Wireshark and built-in tools like Traceroute can support monitoring packets. Quality of Service should be enabled to ensure traffic control is correct and make sure network performance is good.

6.2. Management & Growth

Specialized tools for real-time monitoring can be applied along with backup configurations to reset and restore the network configuration in the case of a severe issue with bandwidth management. Many factors of the configuration can improve such as the bandwidth, device capacity and network design concepts while adding more network devices for expansion and redundancy which improves reliability. Cost must be planned to consider future budgets for required hardware and software, preferably using cost-effective options to save money. All staff within Intercom XP should be trained and aware on the rules and regulations in order to avoid security downsides while educating them on the latest best techniques related to networking.

7. ***Conclusion***

In conclusion, the network configuration of Intercom XP delivers great redundancy and reliable connectivity for both headquarters using access, distribution and core layers.

However, it could always show improvement as the configuration becomes obsolete with outdated technologies while new practices may be introduced for networking.

8. ***Reference List***

- Cisco Press (2014). *Hierarchical Network Design Overview (1.1) > Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design*. [online] www.ciscopress.com. Available at: https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4.

- Stallings, W. (2014). *Data and computer communications*. Harlow, Essex: Pearson.

- Tanenbaum, A.S. and Wetherall, D. (2011). *Computer Networks, Fifth Edition*. Prentice Hall.

- Cisco (2023). *Networking Requirements and Recommendations*. [online] Available at: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/webexcc/desktop_10/webexcc_b_10-desktop-user-guide/webexcc_b_10-cisco-webex-contact-center-agent_chapter_0111.pdf

- Kaeo, M., 2004. *Designing network security*. Cisco Press.