

## CHAPTER 8

# How IT Systems Are Structured

As you might have guessed from the first part of this book, IT Support is a mixture of detective work, diplomacy, technical prowess, and sifting through masses of data on a regular basis. Well, what if I told you that the IT Support you provide can also be affected, or problems created by the natural or built environments in which we live and work?

You probably think I'm mad at this point for suggesting that trees, rivers, and buildings can cause problems with computers and you'd be right. I've never seen a single instance of a computer being adversely affected by a giant oak tree, or disrupted by a horse, but there are instances where our environment needs to be considered carefully.

We'll begin though by looking at our IT systems themselves. How do we structure and build them, what do we expect from them, and we'll look a little more in-depth at the interconnectedness of things that I've mentioned before.

## In the Beginning, the Unix-verse Was Created...

What was your first computer? Mine was a Sinclair ZX81, a small black box about the size of a paperback book that plugged into my television set and a cassette player (remember those?). You could use two (read it, two) accessories including a RAM expansion pack, and a thermal printer (which was utterly epic and once used to print some wedding invitations).

By the time I'd moved to a PC, things hadn't changed very much. My Olivetti M240 had a monitor, keyboard (no mouse, as I used MS DOS and DR DOS at the time), and had a dot matrix printer attached. Indeed I still have some printouts created using WordPerfect 5.1 on that machine.

Now things are very different. As I write this, the peripherals I have connected to my PC include an LG 38-inch curved, ultra-wide monitor, Logitech wired keyboard and wireless mouse, Saitek flight controllers set (for playing *Elite: Dangerous*), an Xbox Elite gaming controller, and a Bose volume knob that sits between the PC and my (also Bose) speakers. Both printers/scanners, a Brother and a Canon, are connected over ethernet and Wi-Fi, respectively.

If I look at the other connected devices on my home office network, there's the broadband modem (obviously) provided by Starlink, a Netgate security appliance (which was recommended to me by a former head of cyber security at GCHQ, Britain's cyber intelligence service), a Netgear Mesh router system with two satellites and three additional wired TP-Link Wi-Fi extenders, one indoors and two outdoors, two NAS drives (one for backing up the first as I'm utterly paranoid about data loss), seven IP security cameras connected to two base stations, various Amazon and Bose Alexa smart speakers and two Bose smart soundbar surround systems, my friend's gaming PC for when he comes to stay, with connected monitor, mouse, and keyboard, My Microsoft Surface laptop Studio, two mobile phones (one really just used for banking and authentication because I don't like taking that one out of the house just in case), four televisions in my garden room (I've banned TV from the living room and prefer to enjoy my Rega turntable, amp and speakers for listening to my vinyl record collection there), two bedrooms, and my gîte (an outhouse common to countryside properties in France), and probably a few other things that have become so ubiquitous that I've forgotten about them.

In addition to this, there are a few IoT (Internet of Things) devices that are controlled through apps, including four monoblock air-conditioning units, two solar panel systems, and there are two washing machines, two ovens, and a dishwasher that all *want* me to connect them to the Internet but that I flatly refuse to do so, firstly because it potentially opens a huge hole in my home IT security, but also because it's just plain dumb. Let's face it, if I want to turn a washing machine on, what would I have just been doing and where am I likely to be stood?

The Netgate security appliance and the Wi-Fi extenders present an interesting case. The Netgate sits between my Starlink router and my Netgear Orbi router so that it can monitor and filter all the traffic coming into and out of my home/office. Also the TP-Link extenders cannot be managed by the Orbi system (so I'm looking at swapping that out for a TP-Link one). All of this adds significant complexity to my network, and any of you

who have had to manage a complex network setup in a workplace will know how it can feel when you're trying to diagnose a network problem, but there are a lot of potential points of failure.

Let's then look at the way IT systems are structured in a typical workplace. You will have multiple, sometimes hundreds of desktop and laptop PCs, dozens of printers and a few document scanners, just about everybody's smartphone will be connected to the company Wi-Fi and you'll likely have at least three or four different networks for that, all operating on different channels and frequencies, and you'll likely have a few tablets knocking around as well. There might be a local file server or NAS drive (or several), and perhaps a local server as well, possibly a holdover for a critical system that's difficult or perhaps even impossible to move to the cloud. There'll be a router, switch and patch boxes, and all the cabling to connect those switch boxes to ethernet sockets, Wi-Fi extenders and all the cabling for those complete with separate PoE (power over ethernet) switches, and possibly a separate management system for them.

All of this equipment is essential to the smooth and daily running of the workplace and they're all interconnected. It's this interconnectedness that can prove to be the Achilles' heel of the system that you have and I'm certainly aware of how hideously complex I've made my own system.

Let's take the example of a large office where there are networking problems. Could this be caused by a switch box, and if so, which one? Could it be caused by a faulty ethernet socket? Could it be caused by damaged or snagged cabling? Could it be the fault of the person who bought unshielded network cable that's now suffering from electrical interference because it runs close to the microwave in the kitchen? In fact it could be caused by *any* of these things and about another 100 things as well.

## IP Freely

No this isn't a joke from the Simpsons but important information about limitations of the current technologies we use. While IPv6 networking has been with us for some years now, it's still the older IPv4 networking system that dominates. This provides a physical limit of around 4.3 billion addresses, and we've long since outstripped that number for Internet- and network-connected devices worldwide.

## РОЗДІЛ 8

# Архітектура ІТ-систем

Як ви могли помітити у першій частині цієї книги, робота в сфері ІТ-підтримки— це поєднання аналітичної роботи, дипломатії, технічної майстерності та регулярного аналізу великих обсягів даних. А що, якби я сказав, що на роботу в сфері ІТ-підтримки може впливати як природне, так і штучно створене середовище, де ми живемо і працюємо?

Ви, ймовірно, думаєте, що я збожеволів, стверджуючи, що дерева, річки та будівлі можуть створювати проблеми для комп'ютерів, і, мабуть, маєте рацію. Я жодного разу не бачив, щоб комп'ютер зазнав проблем через величезний дуб чи вийшов з ладу через коня. Однак бувають випадки, коли вплив середовища потрібно ретельно враховувати.

Проте спершу зосередимось безпосередньо на розгляді наших ІТ-систем. Як ми їх структуруємо і будуємо, які завдання перед ними ставимо, а також детальніше розглянемо взаємозв'язок тих аспектів, про які йшлося раніше.

## Спочатку Був Створений Unix-всесвіт...

Який був ваш перший комп'ютер? Мій був Sinclair ZX81 — невеликий чорний пристрій розміром з книгу в м'якій обкладинці, який підключався до телевізора та магнітофона (пам'ятаєте такі?). Доступними були лише два (так, саме два) додаткові пристрої: модуль розширення оперативної пам'яті та термопринтер (який був неймовірно крутим і одного разу навіть використовувався для друку запрошень на весілля).

Коли я перейшов на ПК, мало що змінилося. Мій Olivetti M240 був обладнаний монітором, клавіатурою (без миші, адже я тоді використовував MS DOS і DR DOS), а також мав підключений матричний принтер. Я досі зберігаю кілька роздруківок, створених на тому комп'ютері за допомогою WordPerfect 5.1.



Наразі все дуже змінилося. На момент написання цього тексту до мого ПК підключені такі периферійні пристрої: вигнутий ультраширокий монітор LG на 38 дюймів (96,52 см), дротова клавіатура та бездротова миша Logitech, набір контролерів Saitek для авіасимуляторів (для гри в Elite: Dangerous), геймінговий контролер Xbox Elite і регулятор гучності Bose, який розташований між ПК та моїми (також Bose) колонками. Обидва принтери/сканери, Brother та Canon, підключені через Ethernet і Wi-Fi, відповідно.

У моїй мережі для домашнього офісу підключені такі пристрої: широкосмуговий модем (звісно) від Starlink, пристрій для захисту мережі Netgate (який порекомендував мені колишній глава кібербезпеки з GCHQ, британської служби кіберрозвідки), система маршрутизаторів Netgear Mesh із двома супутниками та трьома додатковими дротовими Wi-Fi ретрансляторами TP-Link, один у приміщенні, а два інші встановлені зовні, два накопичувачі NAS (другий забезпечує резервне копіювання першого, адже я надзвичайно боюся втрати даних), сім IP-камер спостереження, підключених до двох базових станцій, декілька смарт-колонок Amazon та Bose Alexa, а також два Bose смарт-саундбари з об'ємним звучанням. Є також ігровий ПК мого друга, з підключеним монітором, мишею та клавіатурою, мій ноутбук Microsoft Surface Laptop Studio, два мобільні телефони (один використовується лише для банкінгу та аутентифікації, оскільки я не люблю брати його з дому, щоб уникнути ризику), чотири телевізори в моїй садовій кімнаті (я заборонив телевізор у вітальні і віддаю перевагу слухати свою колекцію вінілових платівок на програвачі Rega зі звуковим підсилювачем і колонками), два телевізори в спальнях і один у гіті (господарському приміщенні, поширеному в сільських районах Франції), а також, мабуть, ще кілька пристроїв, які стали настільки звичними, що я про них забув.

Крім цього, є кілька пристроїв IoT (Інтернет речей), які керуються через додатки, зокрема чотири моноблочні кондиціонери, дві системи сонячних панелей, а також дві пральні машини, дві духові шафи і посудомийна машина, які хочуть, щоб я підключив їх до Інтернету. Однак я категорично відмовляюся це робити — по-перше, це становить серйозну загрозу для домашньої ІТ-безпеки, а по-друге, це просто безглуздо. Чесно кажучи, якби я хотів увімкнути пральну машину, що б я щойно зробив і де б я, найімовірніше, знаходився?

Пристрій для захисту мережі Netgate і Wi-Fi ретранслятори викликають особливий інтерес. Netgate розташований між моїм маршрутизатором Starlink і маршрутизатором Netgear Orbi, забезпечуючи моніторинг і фільтрацію всього трафіку, що проходить через мій дім/офіс. Також ретранслятори TP-Link несумісні з системою Orbi (тому я розглядаю можливість замінити її на систему TP-Link).

Усе це значно ускладнює мою мережу, і ті, хто стикався з налаштуванням складної мережі на робочому місці, розуміють, як складно буває діагностувати проблему, коли є багато можливих точок відмови.

Отже, розглянемо, як ІТ-системи побудовані у типовому робочому середовищі. У вас може бути багато, а то й сотні настільних ПК і ноутбуків, десятки принтерів і кілька сканерів документів. Практично кожен смартфон співробітників підключатиметься до Wi-Fi компанії, що потребуватиме створення трьох-чотирьох різних мереж, працюючих на різних каналах і частотах. А також, швидше за все, буде кілька планшетів у використанні. Можливо, у вас буде локальний файловий сервер або накопичувач NAS (або декілька), а також локальний сервер, імовірно залишений для роботи критично важливої системи, через неможливість її перенесення або функціонування в хмарному середовищі. Також буде маршрутизатор, комутатор і патч-бокси, а також усі кабелі для підключення цих комутаторів до Ethernet-сокетів. Окрім цього, будуть ретранслятори Wi-Fi із відповідними кабелями, забезпечені окремими PoE-комутаторами (подача живлення через Ethernet), а також, ймовірно, окрема система управління для них.

Усе це обладнання є необхідним для безперебійної та щоденної роботи офісу, і всі ці елементи взаємопов'язані. Саме ця взаємопов'язаність може виявитися ахіллесовою п'ятою вашої системи, і я, безумовно, усвідомлюю, якою надзвичайно складною я зробив свою власну систему.

Уявімо великий офіс, де часто виникають збої в роботі мережі. Чи може це бути спричинено комутатором і, якщо так, то яким саме? Чи може це бути спричинено несправним Ethernet-сокетом? Чи може це бути спричинено пошкодженими або перетиснутими кабелями? Чи може проблема виникати через те, що хтось придбав неекранований мережевий кабель (без захисту від електромагнітних перешкод), що знаходиться поряд із мікрохвильовкою на кухні? Можливо, це пов'язано з однією з цих причин або ще з сотнею інших.

## АйПі-шуй Вільно

Ні, це не жарт із мультсеріалу "Сімпсони", а важлива інформація про обмеження сучасних технологій, які ми використовуємо. Хоча мережева система IPv6 існує вже кілька років, домінуючою залишається старіша система IPv4. Фізичне обмеження складає близько 4,3 мільярда адрес, і ця межа була давно перевищена через стрімке зростання кількості пристроїв, які підключаються до мережі та Інтернету у всьому світі.