EBOOK

What's Causing That Ticket?

A Beginner's Guide to Troubleshooting Devices, Networks, and Applications for Service Desk Teams

Contents

Introduction

In today's world, a company's success depends on the quality of the experiences it's able to give its employees. Because these experiences are so tech-dependent, IT support professionals play a huge role in keeping employees happy, satisfied, and productive. Companies simply couldn't operate—let alone grow and thrive—without them. But service desk analysts' jobs are far from easy. Since the pandemic accelerated the adoption of hybrid and remote work, support teams have been busier than ever, with support ticket volumes having increased by 35% since 2020.[1] Given this explosion in ticket numbers, the increasing complexity of IT environments, and the difficulty of recruiting and retaining talent, it's critically important for new hires in this fast-paced field to get up to speed quickly.

To help service desk agents to resolve more tickets faster, we've put together this beginner's guide to the most commonly-encountered issues impacting end user devices, connectivity, and application performance.

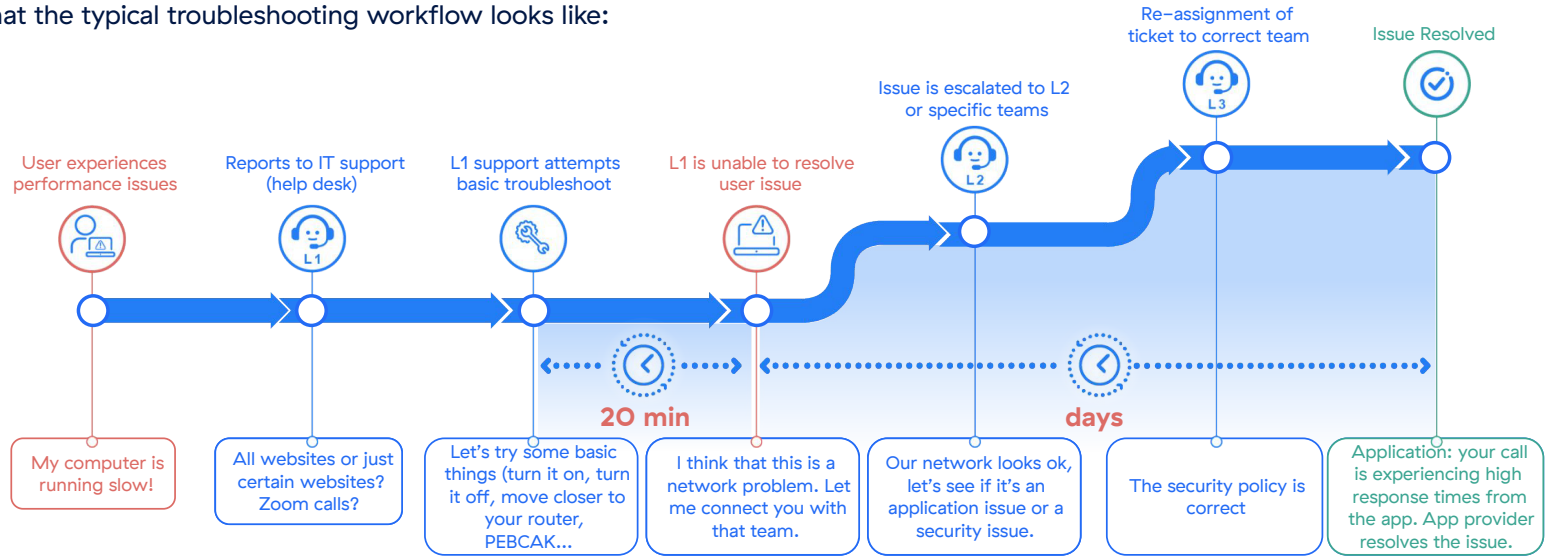
1. "Helpdesk meltdown due to absenteeism, low morale and increased workload," Computer Weekly, February 2021

Resolving Tickets, Step by Step

Depending on their organization's size and industry, service desk teams can expect to field between **979** and **18,331** support inquiries each month.[2]

That's a lot of tickets! Responding to all of them quickly and appropriately (this means deciding which ones can be handled immediately, and which need to be handed off to a higher-level agent) can seem overwhelming at first.

Here's what the typical troubleshooting workflow looks like:



We like to group the most common issues service desk analysts encounter on the job into three categories. These are device issues (problems on the end user side), networking issues (problems connecting the end user to an application), and application issues (problems within a cloud or corporate app). Let's take a closer look at each category.

2. "Ticket escalation: What it is and how to manage it," *Zendesk*, December 2023.

Device Issues

These are all the problems that occur in the end user's home (or at the coffee shop where they're working). This category includes issues with the user's desktop or laptop computer, as well as with their Wi-Fi router and network. Many of these problems can be resolved by rebooting the device or changing how it is configured.

Poor Wi-Fi Connectivity

What the end user will experience: Frequent disconnections from their wireless internet service at home, slow connection speeds, and trouble connecting to applications—all of which can make it hard to get work done.

Wi-Fi Routers: Key Device Metrics

Wi-Fi Device Metric	What This Means	Example
OS Name	Operating system the end user's device is running	Microsoft Windows 10 Pro
Last Start Time	Last time that device was turned on or rebooted	Jan 12, 10AM PST
Username	Who's logged into that device	PC-ALESS-37\admin
City	End user's location	Dublin
State	End user's location	Ohio
Geo	End user's location	United States
Region	End user's location	Dublin, Ohio
Device Time Zone	End user's location	UTC-05:00 America/New_York
Adapter Name	Name of device enabling the end user's computer to pick up Wi-Fi signals	TP-Link Wireless USB Adapter
Client Source IP	End user's IP address	74.133.7.25
Wi-Fi Signal	Strength of Wi-Fi signal end user's device is receiving	100%
SSID	SSID of network they're connected to	3Com_Wifi
Type	Wi-Fi signal type	802.11n
Interface	Name of wireless network interface controller	TP-Link Wireless USB Adapter
Channel	Wi-Fi network channel they're connected to	10
DNS	IP address of DNS server	192.168.7.254
Gateway	IP address of internet gateway	192.168.7.254
Status	Connection status	Connected

What is Wi-Fi?

Wi-Fi is a local networking technology that makes it possible for devices to connect to the internet (and each other, if they're on the same network) without using wires or cables. Wi-Fi networks use radio waves to transmit information, with each device on the network connecting wirelessly to the Wi-Fi router, which, in turn, connects to the public internet. Unlike AM and FM radio stations, which emit signals whose frequencies are measured in megahertz (MHz), Wi-Fi signals are transmitted at frequencies that range from 2.5 to 5 gigahertz (GHz).

Wi-Fi makes it possible for many different types of devices to access the internet, regardless of where they're placed within the home (or library, airport, school, or other public venue). It's more flexible—and often more cost-effective—than wired connectivity infrastructure.

What's an SSID?

A service set identifier (SSID) is a unique sequence of up to 32 characters that's used to name an individual Wi-Fi network. Each wireless router or access point broadcasts its own SSID, making it possible for users to identify the network they want to use, even if multiple wireless networks are available in the same area. The router broadcasts the SSID several times each second to advertise its presence.

Most Wi-Fi routers will have a label with the name of their SSID somewhere on the side, back, or bottom. SSID names can also be found and displayed on Windows, macOS, iOS, and Android devices.

Wi-Fi signal strength

It's no surprise that the signal that a Wi-Fi router broadcasts gets stronger the closer you are to the router. If there's an obstacle between your device and the router—or just too much distance—the signal may not stay strong enough to provide reliable connectivity.

Wi-Fi signals are measured in decibel milliwatts (dBm), which—somewhat confusingly—are expressed in negative values (i.e., there's always a minus sign in front of the number.) The strongest possible signal is around −30 dBm, which means you're probably standing right in front of the router. −50 dBm can be considered excellent signal strength, and −60 dBm is still strong. The lowest signal strength for reliable video streaming is −67 dBm, which represents a minimum value for smooth data exchange. Most applications can still run with −70 dBm, and −80 dBm is the minimum required to make a connection. The end user's device will usually display an icon representing the approximate strength of the Wi-Fi signal with a number of bars.

Types of Wi-Fi signals

There are several standard Wi-Fi signal types, each with its own unique specifications. These include:

- **Wireless B (802.11B):** Routers that support only this standard are no longer being manufactured, but some newer routers still support this standard alongside others. Wireless B can transfer data at a maximum rate of 11mbps, and the signal can be transmitted up to 150 feet. Wireless B operates at the 2.4 GHz frequency range—the same as common household appliances like cordless phones and microwaves. This can lead to interference if the router is too close to them.
- **Wireless G (802.11G):** Wireless G can transfer data as fast as 54 mbps, at the same 2.4 GHz frequency, so it has the same interference issues as Wireless B.
- **Wireless N (802.11N):** This newer and faster technology supports a transfer rate up to 300 mbps with two antennas, though typical speeds are usually around 140 mbps. Wireless N operates at both the 2.4 GHz and 5 GHz frequencies, and Wireless N devices can switch between multiple signals. Wireless N routers are capable of supporting multiple end user devices at the same time, making them a good (and popular choice) for home Wi-Fi networks.
- **Wireless AC (802.11AC):** This technology can support blazingly fast transmission speeds of up to one gigabit per second while providing stronger signals and wider coverage than Wireless N. Wireless AC routers are best for small business use or for use in homes that are too large to cover with a Wireless N router.

Pro Tip:

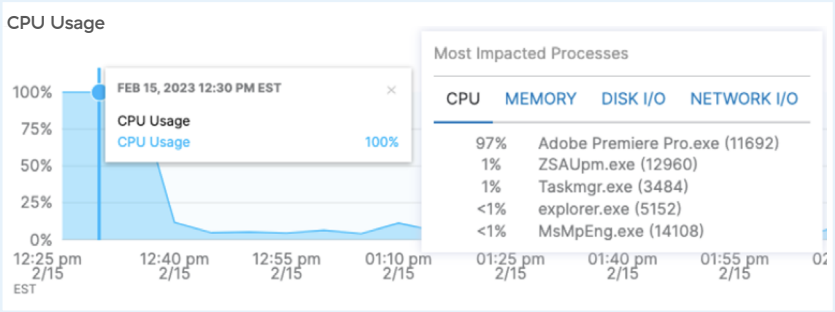
Be on the lookout for changes in Wi-Fi signal type. These changes can indicate that there's an issue causing the connection to slow.

High CPU or Memory Usage

What the end user will experience: Slow device performance, slow application access, or applications crashing. End users may not be aware that their own devices are to blame.

What's a CPU?

The central processing unit (CPU) is the most important chip in any computer. It's like the computer's brain, executing commands to process all the instructions and logic that make the computer work. The CPU also tells other chips and components within the system how to process commands so that the computer can function as a whole.



Each application that runs on an end user's device will send instructions to the CPU, but all of these applications must share the CPU's time and processing power. If any one application is consuming too many of the system's resources (meaning the CPU is occupied with tasks related to that application), it won't be able to support other applications or essential operating system functions that it needs to perform just to keep running.

Operating system tools like Task Manager (Windows) or Activity Monitor (macOS) let you see how many processes are running on that machine, as well as how much CPU time each process is consuming. If a single process is using 100% of the CPU's resources for a short time, that may not cause problems. However, if a process is consistently using too much CPU time, it may make the entire system unstable or cause it to stop working.

What is memory?

Before the CPU can execute instructions, it has to receive them. If all of this data were stored on a hard drive, it would take a long time to reach the CPU, and the computer would run very slowly. Instead, the information is stored on chips close to the CPU, in what's known as random access memory (RAM). The more of this memory that a computer has, the less often it has to access instructions from a storage device or another source. This makes it run faster and perform better.

When a system is low on memory, applications will often run slowly or be unresponsive, since the computer isn't able to send the CPU all the instructions it needs to perform well. Sometimes the solution is as simple as closing background applications so that fewer programs are running at the same time. Other times, the end user's device may need to be reconfigured (adding more virtual memory, for example).

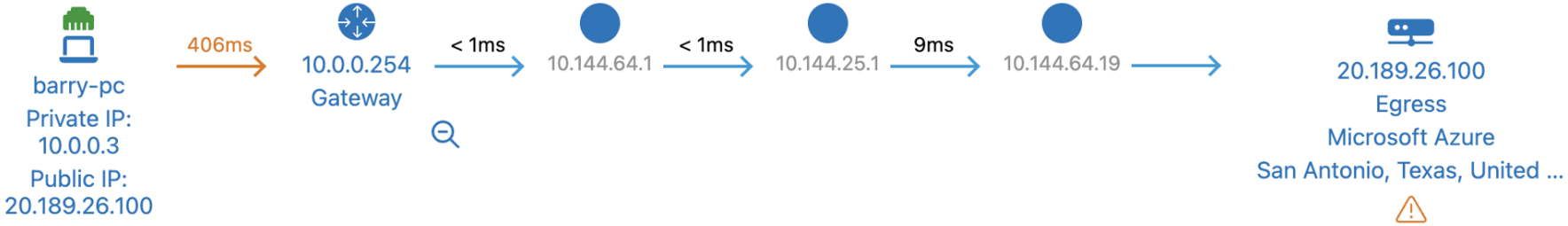
Networking Issues

The data that travels between an end user's device and the application they're using takes many different "hops" as it crosses the corporate network or public internet to reach its destination. Problems can occur at any of the steps along the way, from the servers that power the internet to the routers that direct its traffic. Some of these issues can be resolved by internal IT or networking teams, while others may require the attention of Software as a Service (SaaS) providers or other vendors.

Here's an example of network hops. In this case, the end user's traffic takes 5 steps to reach the destination application.

Pro Tip:

Some applications are internal, so their traffic is routed over a Virtual Private Network (VPN), which adds in extra network hops. These extra hops can cause end users to experience application slowness.



Slow DNS

What the end user will experience: Trouble connecting to SaaS apps. Users might report that Zoom calls are fine once connectivity is established, but everything else on the web is very slow, for instance.

What is DNS?

The domain name system (DNS) is like a map for the entire internet. In essence, it's a database that holds Internet Protocol (IP) addresses—each of which is a set of numbers, like 165.225.80.34—that correspond to the domain names that users type into their browsers. So, for instance, if you type "zscaler.com" into Chrome, a DNS server will map that name onto the corresponding IP address so that it can send your traffic to the right place. This process is called "resolving" the DNS request.

If the nearest DNS server doesn't answer, the browser will then query a series of other servers, which will work together to continue redirecting the request an answer is finally delivered. If any of these servers are not working properly, it can take a long time to reach the destination website, or the end user might get an error message stating that the website they're trying to reach is unavailable. If the process of resolving DNS requests is slow, users won't be able to access the websites and internet resources they need to stay productive.

Resolving a DNS Request

1. The user types a website name into their browser.
2. That browser sends a message to the nearest DNS server (usually the one managed by the internet service provider (ISP)) to find out which IP address corresponds to that website.
3. The end user's browser sends a connection request to the web server at that IP address.
4. The web server responds, establishing the connection.

Slow Network Router

What the end user will experience: Significant slowdowns in page load times when accessing SaaS apps, and often performance will be erratic, with problems that seem to show up at random and then resolve themselves on their own.

What is a router?

Routers are appliances that pass data packets between networks, inspecting each packet to determine its destination and then calculating the most efficient way for it to reach that destination.

There's a near infinite number of possible paths that each packet could take as it travels to this destination, and some are much shorter—and thus faster—than others. When network traffic slows down, it's typically because there's a problem along one segment of the path that the traffic is taking. If there's high latency along a single hop along the data path, application performance and user experience will suffer.

What causes latency?

Some degree of latency—the amount of time it takes for each data packet to travel round-trip to its destination application and back again—is always present. When there's a great deal of latency, web pages load slowly, video and audio stream quality is poor, and user experience suffers.

Packet loss—when a significant percentage of data packets fail to make it to their destination—can introduce latency, as can jitter, which occurs when there's too much variation in the amount of time it takes the different packets within a data stream to reach their destination.

Determining root causes of latency

It can be challenging to figure out which of the many hops that data packets take on their path to the target application and back is the one where the problems are occurring. Network monitoring tools or other diagnostic tests can help to pinpoint the cause of the issue.

Application Issues

Sometimes the problem lies within the SaaS app that employees are trying to access. When service desk teams understand this, they can proactively alert users in case of an outage, and can prepare detailed evidence of the problem to send to the SaaS vendor.

Call Quality Issues on Microsoft Teams, Zoom, or WebEx

What the end user will experience: Poor call quality and meeting experiences when using collaboration and communication apps. These issues often occur sporadically, making troubleshooting especially difficult.

What are UCaaS apps?

Unified communications as a service (UCaaS) applications include many different capabilities like chat and online messaging, virtual meetings, telephony, videoconferencing, and content sharing. These apps support collaboration by making synchronous and asynchronous team communications possible across a wide variety of devices. The apps typically run on servers hosted by UCaaS providers in their own data centers or on public cloud platforms. End users can download software clients onto their devices or use phones or videoconferencing equipment that's been configured to work with the UCaaS provider's systems.

UCaaS apps exchange an array of different data types, from chat text streams to audio and video streams. To understand what's causing the problem, UCaaS monitoring tools need to collect detailed information on each of these data sources, down to the level of the individual end user's experience. This enables them to detect the factors contributing to poor experiences, even if they aren't consistent across different users or meetings.

Pro Tip:

Not everyone using the same UCaaS app (e.g., Zoom, Microsoft Teams, WebEx) will experience the same issues. First, figure out which individuals are impacted. Then, dive into analyzing their experiences.

Slow Application Response Times

What the end user will experience: An application (such as Chrome, Microsoft SharePoint, or SAP) isn't responding or won't run.

What's an application?

A software application is a program or group of programs that performs a specific function for its users. Applications that run on end user devices are supported by those devices' operating systems; those that run on a server in the cloud are accessed through a web browser and may not have access to the end user's device.

Applications can crash (stop running) if one of their components encounters an error that it wasn't programmed to handle. They can also stop responding even when they're still running, perhaps because they're stuck waiting for a response that they're not getting or because there isn't enough available memory. These sorts of failures can occur in applications running on an end user's device or in those running in the cloud. SaaS vendors typically build many fail-safe measures into their products to reduce downtime, so cloud application outages aren't all that common. But they do occur.

What is application response time?

Application response time is the average amount of time it takes to display the entire contents of a web page in your browser. It's calculated from the instant that you click on a link or type in a domain name to the point at which the page is fully loaded. Page load times are measured in seconds, and the faster they are, the better users' experiences will be.

What Is TTFB?

HTTP Request Time + Process Request Time + HTTP Request Time = TTFB

Often called Time to First Byte (TTFB), server response time is the amount of time it takes a server to respond to a request. Faster server response times are always better, providing users with a sense of immediate gratification and removing performance bottlenecks.

Pro Tip:

Some applications are internal, so their traffic is routed over a Virtual Private Network (VPN), which adds in extra network hops. These extra hops can cause end users to experience application slowness.

Improving Troubleshooting Workflows

On the market today, there are many different solutions—including combinations of point products—that service desk analysts can use to figure out the root causes of issues so that they can help employees get back to work quickly and meet service level agreements (SLAs).

Not all of these tools are created equal, though. Some leverage advanced technologies like AI to correlate data from multiple sources, including home Wi-Fi networks, ISPs, and applications, to automatically determine the root causes of issues. Solutions that allow service desk analysts to drill down into incident details (such as type, severity, start and end times, and duration) are more helpful, since they can give you a full and nuanced understanding of the issue.

Look for a monitoring solution that can:

- Provide complete visibility, showing the causes of multiple different types of issues in just one place
- Decrease learning time by providing an intuitive, easy-to-use dashboard
- Offer AI assistance to make it easier to identify root causes quickly
- Provide insights that empower you to take a proactive approach to issues like application outages
- Integrate with the ITSM tools you already use, so that it's easy to track tickets, share documentation, and forward key information to other members of your team

Pro Tip:

Some of today's most advanced digital experience monitoring solutions include self-service capabilities. This means they can tell end users how to fix issues like poor Wi-Fi connectivity or excess CPU utilization on their own, so that service desk agents don't even need to get involved.

Introducing ZDX

Modern enterprise networks were complex even before hybrid and remote work were widely adopted. Today's IT support professionals are seeing more tickets—and more issues caused by things outside the company's control—than ever before. The good news is that intelligent digital experience monitoring technologies can restore the visibility and control that service desk analysts need to make well-educated decisions, address problems proactively, and close tickets faster.

Zscaler Digital Experience (ZDX) is an intelligent digital experience monitoring solution that continuously monitors applications from an end user perspective to give deep insights into the causes of device, network, and application performance issues. ZDX provides end-to-end visibility and AI-powered troubleshooting intelligence for any user or application, no matter where they're located. It continuously collects and analyzes metrics such as application availability, response times, hop-by-hop network performance, and end user device health. With powerful tools like ZDX at hand, service desk teams can spend less time feeling puzzled or frustrated, and more time helping people and delivering results with a smile.

Learn more

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE—based Zero Trust Exchange is the world's largest inline cloud security platform. To learn more, visit **www.zscaler.com**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com