Vicens Ferran Rabassa
Senior Network Engineer and System Administrator
Cisco Certified Network Professional Enterprise

NETWORK TROUBLESHOOTING

A Practical Guide for Network Technicians in Production Environments

🧠 **Prepared by:** Vicens Ferran Rabassa Specialist in networks and systems.

🗓️ **Publication Date:** September 2025

🔍 **Featured content:**
Structured step-by-step action plan
Diagnostic tools and corrective actions
Communication strategies
Incident Report Template
Troubleshooting checklist
Prevention recommendations

✨ I hope you find this document useful, enlightening, and applicable.
📣 If you found it interesting, like it above and follow me for more technical content:
🔗 www.linkedin.com/in/vicens-ferran-rabassa

NETWORK TROUBLESHOOTING

Initial note

📌 *This document reflects my personal view on troubleshooting LANs in production environments. It is not intended to be an absolute truth, but a practical guide based on experience and technical criteria. It is designed especially for students of telematics networks, as well as for those preparing for certifications such as* **CCNA** *and* **CCNP**. *I hope you find it useful as a starting point, reflection or training reinforcement.*

🧩 Introduction

🗣️ When a LAN network in production fails, time becomes a scarce resource and pressure increases exponentially. Both users and department managers expect a fast, clear and effective solution. In this context, the network technician must not only master technical knowledge, but also maintain an analytical, serene and methodical mindset. In addition, they must have **solid communication skills**, capable of transmitting peace of mind to users and confidence to bosses, adapting the message according to the profile of the receiver and the moment of the crisis.

🔧 **Network troubleshooting is not just about applying orders or looking at logs.** It is knowing how to think like a researcher: formulating hypotheses, validating them with evidence, ruling out causes and narrowing down the problem. The key is **to segment the network**, divide it into smaller parts and progressively isolate the affected areas until the source of the problem is located.

🧠 The technician must know the layers of the OSI model, the protocols involved (TCP/IP, ARP, DHCP, STP...), and be skilled with tools such as **ping, traceroute, SNMP, Wireshark, SSH/Telnet**, among others. But it is just as important to know how to **communicate clearly**, both with users and with superiors, keeping them informed without generating alarm.

⚠️ In times of crisis, emotional pressure can be high. Users may show frustration, bosses may demand immediate results, and every minute of a drop can mean economic or operational losses. It is in these moments that the coach must show a **leadership attitude**, making decisions with confidence, guiding the process clearly and transmitting confidence to the whole team. This attitude not only facilitates the resolution of the problem but also reinforces professional credibility. Therefore, it is necessary to act calmly, **judiciously and confidently**, following a structured plan that allows the service to be recovered and the incident documented to prevent future recurrences.

This article presents my vision of an approach to an **action plan**, designed to help technicians deal with network collapses with rigor, efficiency and serenity. Because in the world of networking, every detail counts – and every decision can make the difference between chaos and recovery.

🧭 1. Emotional control and initial communication

🔹 **They stay calm:** Serenity breeds confidence.

🔹 **Communicate to users:**

"We are solving a network incident. We will keep you updated periodically."

🔹 **Inform those responsible:**

"We have activated the diagnosis protocol. I will inform you every 30 minutes with the current status."

🗣️ 2. Collection of User Information

🔸 Question:

- When did the problem start?
- What services fail (web, email, apps)?
- Does it affect all users or just some?
- Think about any technical information related to the incident and try to find out as much information about it as possible.

🔸 Record patterns:

- Physical location
- VLAN or Network Segment
- Device Type and Operating System

🖥️ 3. Monitoring System Review

🔍 Use monitoring tools such as **Zabbix, PRTG, Nagios, SolarWinds** to detect anomalies if you have them installed, if not, you may have to think about muntar.ne one. If you don't have it, you'll have to review logs of affected devices, for example.

📊 Check:

- Traffic graphs and CPU/memory usage
- Critical Alerts
- Historical logs
- Availability of services (ping, SNMP, HTTP...)

📎 Helpful Resources:

- Zabbix Templates
- Nagios Exchange

🔍 4. Technical diagnosis.

🧠 **Objective:** To identify the probable cause of collapse using diagnostic tools, symptom observation and active checks.

It consists of identifying the cause of the problem by analysing symptoms, segmenting the network, and checking protocols, routes, and configurations. You must think like a researcher and progressively isolate the affected areas.

🛠️ Recommended and common diagnostic tools

They are tools that allow you to analyse traffic, device status, configurations and detect anomalies in real time.

🔹 **ICMP (ping, traceroute):** Allows latency, packet loss, and unreachable paths to be detected.

🔹 **SNMP (Simple Network Management Protocol):** Checks the status of network devices (switches, routers, APs) and collects data such as:

- CPU and memory usage
- Interface Saturation
- Traffic errors
- Port status

📎 *Useful resource:* LibreNMS – Free and powerful SNMP monitoring.

🔹 **SSH / Telnet connections:** Direct access to devices for:

- Consult logs
- Execute diagnostic requests (show interfaces, show mac address-table, show ip route, etc.)
- Verify configurations (ACLs, Vlans, STP, routing)

🔹 **Wireshark/tcpdump:** Packet capture to detect:

- Anomalous traffic
- Suspicious protocols
- Relay cycles or loops

🔹 **System and device logs:** Review events such as:

- Ports that change state
- STP errors
- Buffer saturation
- Packet rejection

📊 Technical Diagnosis Table

In this table there is a summary of some technical incidents that can occur and how to deal with them.

🧩 Problem	🧬 OSI Layer	🔎 Typical symptoms	🧪 Initial Action
🌪️ Broadcast storm	2	Massive traffic, saturated switches, flashing LEDs	Disconnect suspicious segments, check STP
🔁 Network loops (without STP)	2	Circular traffic, congestion, loss of connections	Activate STP, verify physical topology
🦹 ♌ MAC flooding / ARP spoofing	2	Erratic traffic, full MAC tables, unstable connections	Analyse ARP/MAC tables, capture with Wireshark
🧨 DHCP Spoofing	2	Incorrect IPs, limited or no access	Disable suspicious ports, check DHCP logs
🧭 Misconfigured routing	3	Traffic that does not arrive, inaccessible routes	Review routing tables with SSH/Telnet
🧮 Incorrect Summarization	3	Subnet conflicts, erroneous routes	Review Routing Design and Summarization
🚫 Poorly defined ACLs	3	Blocking legitimate traffic	Review access lists with SSH/Telnet
🔥 Firewalls with Bad Policies	3	Isolated areas, blocked services	Review Firewall rules and logs
🧱 Defective device	2/3	Anomalous traffic from a host, spot saturation	Physically isolate the device, analyse with SNMP
📦 P2P Applications / Backups	2/3	High traffic at peak times, general slowness	Review traffic logs, SNMP, and packet captures

✅ Good Practices:

To ensure efficient and safe troubleshooting on LAN networks, it is advisable to follow recognized regulations and frameworks. Standards such as ***ISO/IEC 27001***, ***ITIL*** or the ***Cisco Troubleshooting Guidelines*** that offer structured methodologies and practical tools. These models facilitate traceability, communication, and continuous improvement**.**

🧩 Top Areas Covered by Cisco Troubleshooting Guidelines

🔹 1. Layered Diagnosis

Cisco recommends following the OSI model to address network issues, starting with the physical layer and progressively working your way up:
- Layer 1 (Physics): Verification of cables, ports, signal.

- Layer 2 (Data Binding): Review of MAC, STP, Vlans tables.
- Layer 3 (Network): Routing, IPs, Summarization, ACLs.

🔹 2. Essential Controllers

Cisco proposes to use a series of commands to troubleshoot devices such as switches and routers, such as, among others:
- **Ping** and traceroute: to verify connectivity.
- **Show Interfaces**, Show IP Route, Show Mac Address-Table: to analyse status and traffic.
- **Debug** (with caution, not advised in production): to track behaviour in real time.

🔹 3. Common LAN switching issues

Cisco's official documents include guides to resolve:
- Speed and duplex self-negotiation issues.
- Errors in ISL/802.1Q trunking.
- EtherChannel configuration and diagnosis.
- Incidents with Spanning Tree Protocol (STP).
- Connectivity issues of end stations (PortFast, BPDU Guard).

🔹 4. Multilayer switching

Cisco also addresses configuration and troubleshooting in environments where switches operate at Layer 2 and Layer 3, including:
- Internal routing in switches.
- Inter-VLAN routing.
- Security and access control policies.

📚 **Official Cisco Resources**

- Official PDF Guide: Troubleshooting LAN Switching Environments
- Web Documentation: Cisco LAN Switching Troubleshooting
- Community Article: Cisco Community Troubleshooting LAN Switching

🛠️ 5. Corrective actions

Once the problem is located, measures such as isolating devices, reconfiguring routes, reviewing ACLs or restarting computers must be applied. The goal is to restore the minimum functionality of the network quickly and securely.

🔧 Segment the network to locate the focus
🔧 Isolate suspicious devices
🔧 Reconfigure routing protocols
🔧 Check ACLs and firewalls
🔧 Restart computers if they don't respond.

📣 6. Ongoing communication

It is key to keep both users and managers informed. You must adapt the message according to the profile, convey tranquillity and always show leadership to reinforce confidence.

📢 User Updates:

"The network is in the process of recovery. We will inform you when it is fully operational."

📢 Reports to superiors:

"We have identified the probable cause. We are implementing corrective measures. We estimate partial recovery in X minutes."

🗂️ 7. Incident Documentation

The chronology, tests performed, solution applied, and impact must be recorded. This documentation is essential for further analysis, internal training and prevention of future incidents.

📝 Records:

- Chronology
- Symptoms
- Hypotheses and tests
- Solution applied
- Impact
- Lessons learned
- Monitoring System Screenshots

📎 Helpful Resources:

- RFC 2544 – Benchmarking Methodology
- Wireshark Display Filters

✅ 8. Recovery and prevention

After the problem is resolved, technical improvements, audits, and training must be implemented. The objective is to strengthen the infrastructure and minimize the risk of recurrence, thinking about continuous improvement and productivity.

🔒 Security
📚 audit User
📏 training technical improvements: Vlans, QoS, port
🧠 control Simulation of future incidents

📎 Helpful Resources:

- Cisco Packet Tracer or other emulators.
- LibreNMS

📎 9. Sample Documents

📝 Network Incident Report Template Example

Title of the incident: 🔹 *(Ex: VLAN 20 crash in building B)*
Start date and time: 🗓️ *(Ex: 04/09/2025 – 09:42h)*
Date and time of resolution: 🗓️ *(Ex: 04/09/2025 – 11:15h)*
Responsible technician: 👤 *(Name and surname)*
Description of the problem: 📄 *(Brief summary of what happened, symptoms observed, services affected)*
Affected area or segment: 📍 *(Ex: VLAN 20 – Floor 2 – Building B)*
Impact: ⚠️ *(Number of users affected, services down, operational impact)*
Diagnosis made: 🔍 *(Tools used, tests performed, hypotheses discarded)*
Cause identified: 🧠 *(Ex: Network loops due to STP disabled on a new switch)*
Corrective actions applied: 🔧 *(Ex: STP activation, switch reboot, Vlans reconfiguration)*
Communication carried out: 📣 *(Messages sent to users and managers, channels used)*
Attached documentation: 📁 *(Screenshots, logs, monitoring graphs, etc.)*
Lessons learned/preventive actions: ✅ *(Ex: Review STP configuration on new devices, pre-deployment checklist)*

✅ Example of a Checklist for LAN Troubleshooting

- ☐ Staying calm and taking leadership
- ☐ Communicate the incident to users and managers
- ☐ Collect information from affected users
- ☐ Identify patterns (location, VLANs, devices)
- ☐ Review monitoring system (Zabbix, PRTG, etc.)
- ☐ Use ICMP tools (ping, traceroute)
- ☐ Querying devices via SNMP
- ☐ SSH/Telnet login to review configurations
- ☐ Capture traffic with Wireshark if needed
- ☐ Verify Vlans, STP, ACLs, routing configuration
- ☐ Isolate suspicious devices or network segments
- ☐ Apply corrective actions
- ☐ Communicate the evolution of the resolution
- ☐ Document the entire process

☐ Propose preventive actions and improvements

📃 10. Final summary

This document has sought to offer a clear, structured and practical vision on how to deal with a LAN network collapse with technical criteria, serenity and leadership. We have reviewed the key phases of troubleshooting, the essential tools, corrective actions and the importance of communication and documentation.

🔍 Segmenting, isolating, and analysing are critical actions to solve complex problems effectively.

🧠 The combination of technical knowledge, analytical attitude and communication skills is what makes a good technician a benchmark in the face of crises.

✨ I sincerely hope that this document has been **clarifying and useful to you**, and that it will serve as a support guide in critical moments or as a basis for training other professionals.

🙌 Did you like the content?

💬 *If you liked the content, you could express it at the bottom of the post and follow me to discover more resources, reflections and technical content on networks and systems.*

🔗 *You will find me on LinkedIn here:* http://www.linkedin.com/in/vicens-ferran-rabassa