How a LAN Audit can improve network performance

A LAN Audit will provide an up to date view of the IT infrastructure, identifying problem areas & providing complete documentation of layer 2/3 topology.

Benefits

- Gain an **understanding** of exactly what devices are present in your network and where.
- Improve **resiliency** through identifying single points of failure and verification of network devices.
- Document the current state of the **network** prior to a data centre migration.
- Identify physical and logical issues affecting service **performance**.

How our solution works

A LAN Audit is a detailed analysis of the current infrastructure present in the organisation and takes the form of both human inspection and automated discovery. Data cabinets and cabling are examined for any physical issues and the location of all network devices is logged.

The automated discovery tool scans the network infrastructure using SNMP and ICMP and reports on responding devices, tracing connections via protocols such as CDP and using ARP tables. This in conjunction with the human inspection is used to create physical and logical diagrams of the network topology including routing and cabling.

Device OS versions are examined to identify known bugs/vulnerabilities and network configurations are checked to ensure requirements such as security policies are implemented. Areas of weakness such as single points of failure or unpatched equipment are highlighted and recommended remedial action provided.
Solution in detail

**Key Benefits and Features**
- **Reduce your infrastructure costs**
  Understand what devices are critical to your business and where resources are being wasted. Reconfiguration or redeployment of devices can see significant improvements in performance without the need to purchase further equipment or upgrades.
- **Improve resiliency**
  Identify single points of failure within the network and take appropriate action to mitigate service outages by implementing fail-over where necessary to protect mission critical services.
- **Improve uptime**
  Identify devices with known software bugs to allow suitable upgrades to be applied eliminating such issues as memory leaks or crashes.
- **Improve security**
  Identify vulnerable services which do not meet current security policies.
- **Improve application performance**
  By removing performance bottlenecks within the infrastructure applications can run faster and user productivity will increase.
- **Speed up migration of services**
  By knowing exactly what devices are within your network and how they are configured you can significantly reduce the time taken to migrate services away from the current data centre.

**Service**
- **Reduced downtime**
  By optimising your existing infrastructure and eliminating single points of failure and unpatched devices network uptime will be improved.
- **Customer workshop**
  Our LAN audit services come with a customer workshop allowing any identified issues to be analysed and remedial action to be recommended.
- **Remedial Action**
  Where issues are identified our consultants can provide expert-level assistance in correcting the issue.
- **Complete visibility of the network infrastructure**
  Know exactly where your network infrastructure is and how it is connected to improve future capacity upgrades by targeting known weak points.
- **Removal of unauthorised network devices**
  Our LAN audit can identify unauthorised network devices such as wireless access points which could cause significant security issues within the business. These devices can be traced and removed.

**Pricing structure**
From £7,100 depending on the number of devices to be audited.
How LAN Audit works

IT infrastructure is discovered through an automated network analyser and equipment is also inspected via an experienced consultant. All findings are documented and presented in a comprehensive report.

- Site visit and installation of discovery tool
- Automated discovery via SNMP/ICMP
- Equipment inspection and documentation
- Gather equipment statistics
- Examine connectivity/cabling

- Understand current capacity
- Identify vulnerable services
- Identify single points of failure
- Identify security issues
- Understand application flows

- Prioritise key findings
- Present detailed layer 2/3 diagrams
- Present network device information
- Illustrate areas of issue
- Recommendations
- Draw conclusions

Discover  ➔  Analyse  ➔  Report