

5.7 Physische Messgeräte - Werkzeuge zur Fehleranalyse

Softwarewerkzeuge zeigen, wie Betriebssysteme, Netzwerkgeräte und Anwendungen einen Fehler wahrnehmen. Physische Messgeräte untersuchen dagegen Kabel, Steckverbindungen, elektrische Signale, optische Signale, Funkstörungen und die tatsächliche Stromversorgung.

Sie werden benötigt, wenn beispielsweise:

- eine Verbindung trotz korrekter Konfiguration instabil bleibt,
- ein Port keinen Link aufbaut,
- Fehlerzähler kontinuierlich steigen,
- Power over Ethernet nicht zuverlässig funktioniert,
- eine Glasfaserverbindung zu hohe Dämpfung aufweist,
- eine Netzwerkdose nicht eindeutig zugeordnet werden kann,
- ein WLAN durch nicht sichtbare Funkquellen gestört wird,
- ein Server über das normale Netzwerk nicht mehr erreichbar ist,
- ein Kabel- oder Hardwarefehler von einem Konfigurationsfehler getrennt werden muss.

“ Ein Messgerät liefert Messwerte und Beobachtungen. Die Ursache ergibt sich erst aus der Verbindung zwischen Symptom, Messpunkt, Referenzwert, Vergleichsmessung und technischer Dokumentation.

1. Sicherheits- und Freigaberegeln

Vor jeder physischen Messung müssen geklärt werden:

- Darf die Verbindung unterbrochen werden?
- Handelt es sich um eine produktive Verbindung?
- Besteht eine redundante Verbindung?
- Kann das Abziehen eines Kabels einen Failover auslösen?
- Wird über das Kabel gleichzeitig Strom übertragen?
- Handelt es sich um Kupfer, Glasfaser oder eine andere Leitung?
- Ist das Messgerät für den Anschluss und den Messbereich geeignet?
- Muss persönliche Schutzausrüstung verwendet werden?
- Sind elektrische Arbeiten einer Elektrofachkraft vorbehalten?
- Können durch die Messung vertrauliche Daten erfasst werden?
- Muss der ursprüngliche Zustand fotografiert oder dokumentiert werden?
- Ist eine Änderung oder Wartungsfreigabe erforderlich?

Grundregeln

- Kabel und Module vor dem Entfernen eindeutig kennzeichnen.
- Vorher- und Nachher-Zustand dokumentieren.
- Nur geeignete und unbeschädigte Messleitungen verwenden.
- Messgeräte nicht ungeprüft an unbekannte Spannungsquellen anschließen.
- Glasfaserstecker nicht mit bloßem Auge betrachten.
- Aktive Glasfaser kann unsichtbare Laserstrahlung führen.
- Optische Anschlüsse vor dem Verbinden inspizieren und erforderlichenfalls fachgerecht reinigen.
- Multimeter nur durch dafür qualifizierte Personen und im zulässigen Einsatzbereich verwenden.
- Produktive Leitungen nicht ohne Prüfung mit einem Tongenerator, Kabeltester oder Loopback-Stecker verbinden.
- Messergebnisse zusammen mit Zeitpunkt, Messpunkt, Geräteeinstellung und Grenzwert dokumentieren.

2. Sichtprüfung vor dem Einsatz eines Messgeräts

Eine systematische Sichtprüfung kann bereits viele Fehler erkennen.

Zu prüfen sind:

- geknickte oder gequetschte Kabel,
- beschädigte Isolierung,
- zu enge Biegeradien,
- Zugbelastung,
- beschädigte Rastnasen,
- lockere Steckverbindungen,
- verschmutzte Anschlüsse,
- verbogene Kontakte,
- ungeeignete Kupplungen oder Adapter,
- Korrosion,
- Feuchtigkeit,
- übermäßige Wärme,
- beschädigte Patchfelder,
- unvollständige Auflegung,
- falsche Beschriftung,
- falsch eingesetzte Transceiver,
- unterschiedliche Fasertypen,
- ungeeignete Patchkabel,
- blockierte Lüftungsöffnungen,
- ausgefallene Lüfter,
- Warnanzeigen an Netzteilen oder Geräten.

LED-Anzeigen einordnen

Anzeige	mögliche Bedeutung
keine Link-LED	kein Signal, Gegenstelle aus, falsches Medium, Kabel- oder Portfehler
Link vorhanden, keine Aktivität	keine Datenübertragung oder nur momentan kein Verkehr
ständig hohe Aktivität	starke Auslastung, Schleife, Broadcastlast oder normaler hoher Verkehr
orange beziehungsweise gelbe LED	herstellerabhängig: Geschwindigkeit, Warnung, Blockierung oder Fehler
wechselnde Farben	herstellerabhängiger Status oder ausgehandelte Geschwindigkeit
PoE-Fehleranzeige	Leistungsbudget, Klassifizierung, Kurzschluss oder inkompatibles Gerät

“ LED-Farben und Blinkmuster sind nicht herstellerübergreifend standardisiert. Ihre Bedeutung muss in der Dokumentation des konkreten Geräts geprüft werden.

3. Ersatzkabel bekannter Qualität

Ein geprüfetes Ersatzkabel ist eines der wichtigsten Diagnosemittel.

Es eignet sich für den kontrollierten Vergleich von:

- Patchkabeln,
- USB-Kabeln,
- Konsolenkabeln,
- Stromkabeln,
- Glasfaser-Patchkabeln,
- DAC-Kabeln,
- Adapterkabeln.

Das Ersatzkabel muss:

- zum Anschluss passen,
- für die benötigte Geschwindigkeit geeignet sein,
- die erforderliche Kategorie oder Spezifikation erfüllen,
- die richtige Belegung besitzen,
- bei Glasfaser den richtigen Fasertyp und Steckertyp verwenden,
- bei USB Datenübertragung und nicht nur Laden unterstützen,
- selbst geprüft und eindeutig gekennzeichnet sein.

Vorgehensweise

1. Ausgangszustand dokumentieren.
2. betroffene Verbindung eindeutig bestimmen.
3. nur das verdächtige Kabel austauschen.
4. alle übrigen Komponenten unverändert lassen.
5. Funktion erneut prüfen.
6. ursprüngliches Kabel bei Bedarf separat testen.
7. Ergebnis dokumentieren.

Einordnung

Ergebnis	mögliche Schlussfolgerung
Fehler verschwindet mit Ersatzkabel	ursprüngliches Kabel oder dessen Steckkontakt ist verdächtig
Fehler bleibt unverändert	Ursache liegt möglicherweise an Port, Gerät, Konfiguration oder weiterem Leitungsweg
Fehler tritt nur bei Bewegung auf	Kabelbruch, Steckkontakt oder Zugbelastung möglich
niedrigere Geschwindigkeit funktioniert	Signalqualität, Kabelkategorie, Adernpaar oder Transceiver möglich
Ersatzkabel funktioniert nur an anderem Port	Port- oder Konfigurationsproblem möglich

“ Ein funktionierendes Ersatzkabel beweist nicht automatisch, dass die gesamte feste Gebäudeverkabelung fehlerfrei ist.

4. Einfacher Kupfer-Kabeltester

Ein einfacher Kabeltester prüft vor allem die elektrische Verbindung und die Aderzuordnung eines Kupferkabels.

Typische Prüfungen sind:

- Durchgang,
- Unterbrechung,
- Kurzschluss,
- vertauschte Adern,
- gekreuzte Adern,
- Split Pair,
- Schirmverbindung,
- Länge oder ungefähre Fehlerentfernung bei höherwertigen Geräten.

Typische Fehlerbilder

Messergebnis	Bedeutung
--------------	-----------

Open	mindestens eine Ader ist unterbrochen
Short	unerwünschte elektrische Verbindung zwischen Adern
Reversed	Adern eines Paares sind vertauscht
Crossed	Adern beziehungsweise Paare sind falsch zugeordnet
Split Pair	Pinbelegung kann logisch richtig erscheinen, aber die Adern stammen aus falschen verdrehten Paaren
Shield Open	Schirmverbindung ist unterbrochen
Length Error	gemessene Länge oder Fehlerentfernung ist unplausibel

Grenzen eines einfachen Kabeltesters

Ein bestandener Wiremap-Test bestätigt nicht automatisch:

- die geforderte Kabelkategorie,
- ausreichende Signalqualität,
- geringe Dämpfung,
- ausreichende Nebensprechdämpfung,
- fehlerfreien Betrieb bei hoher Datenrate,
- zuverlässige PoE-Übertragung unter Last,
- korrekte Qualität aller Steck- und Anschlussstellen.

Ein Kabel kann bei 100 Mbit/s funktionieren und bei 1, 2,5, 5 oder 10 Gbit/s fehlschlagen.

5. Verification, Qualification und Certification

Bei Kupferverkabelung müssen drei Prüfklassen unterschieden werden.

Prüfklasse	Zweck	typische Aussage
Verification	Verdrahtung und grundlegende physische Fehler prüfen	Adern korrekt verbunden oder Fehler vorhanden
Qualification	Eignung für bestimmte Netzwerktechnik untersuchen	Verbindung unterstützt wahrscheinlich eine bestimmte Ethernet-Anwendung
Certification	Verkabelung gegen definierte Norm- und Kategoriegrenzen messen	Permanent Link oder Channel besteht beziehungsweise besteht nicht

Verification

Geeignet für:

- schnelle Fehlersuche,
- Wiremap,
- Kabellänge,

- Kurzschluss,
- Unterbrechung,
- Split Pair,
- Zuordnung einer Leitung.

Qualification

Kann zusätzlich untersuchen:

- mögliche Netzwerkgeschwindigkeit,
- Signalqualität,
- Paketübertragung,
- Linkfähigkeit,
- teilweise PoE-Eigenschaften.

Certification

Ein Kabelzertifizierer misst abhängig von Norm, Adapter und Messaufbau unter anderem:

- Wiremap,
- Länge,
- Einfügedämpfung,
- Laufzeit,
- Laufzeitunterschied,
- Gleichstromwiderstand,
- Widerstandsunsymmetrie,
- Near-End Crosstalk,
- Power Sum NEXT,
- Return Loss,
- Attenuation-to-Crosstalk Ratio,
- Alien Crosstalk bei entsprechenden Prüfungen.

“ Ein einfacher Kabeltester ersetzt keinen normgerechten Kabelzertifizierer.

6. Kabelzertifizierer

Ein Kabelzertifizierer wird verwendet, wenn nachgewiesen werden muss, ob eine installierte Verkabelung eine bestimmte Kategorie, Klasse oder Anwendung erfüllt.

Vor der Messung müssen festgelegt werden:

- Kupfer- oder Glasfasermessung,
- Verkabelungsstandard,
- Kabelkategorie,

- Permanent Link oder Channel,
- verwendete Adapter,
- erwartete NVP,
- geschirmte oder ungeschirmte Verkabelung,
- Grenzwert,
- Anschlussbezeichnung,
- Messrichtung,
- Kalibrierungsstatus des Geräts.

Permanent Link und Channel

Messaufbau	umfasst typischerweise
Permanent Link	fest installierte Verkabelung zwischen den Anschlussstellen
Channel	gesamte Übertragungsstrecke einschließlich Patchkabeln und Steckverbindungen

Die Messergebnisse verschiedener Aufbauten dürfen nicht ohne Berücksichtigung der verwendeten Adapter und Grenzwerte miteinander verglichen werden.

Bei einem fehlgeschlagenen Test dokumentieren

- betroffene Leitung,
- verwendeter Standard,
- Messaufbau,
- fehlgeschlagener Einzelwert,
- Grenzwert,
- Abstand zum Grenzwert,
- Fehlerentfernung,
- Messrichtung,
- verwendete Adapter,
- Datum der letzten Kalibrierung,
- gespeicherten Messbericht.

Typische Ursachen eines nicht bestandenen Zertifizierungstests

- schlechte Auflegung,
- zu weit aufgedrehte Adernpaare,
- ungeeignete Anschlussmodule,
- beschädigtes Kabel,
- zu große Kabellänge,
- ungeeignete Patchkabel,
- schlechte Schirmung oder Erdung,
- falsche Messadapter,
- falscher Messstandard,
- Störungen durch benachbarte Leitungen,

- ungeeignete Kombination verschiedener Komponenten.

7. TDR für Kupferleitungen

Ein Time Domain Reflectometer sendet einen Impuls in eine Leitung und wertet Reflexionen aus. Dadurch können Änderungen der elektrischen Eigenschaften entlang eines Kabels lokalisiert werden.

Ein TDR kann je nach Gerät Hinweise liefern auf:

- Leitungsende,
- Unterbrechung,
- Kurzschluss,
- Beschädigung,
- schlechte Verbindung,
- Impedanzänderung,
- Abzweigung,
- ungefähre Entfernung zur Fehlerstelle.

Vereinfachtes Prinzip

Messgerät

→ elektrischer Impuls

→ Ausbreitung im Kabel

→ Reflexion an einer Störstelle

→ Berechnung der Entfernung aus der Laufzeit

Die Entfernungsberechnung hängt von der Ausbreitungsgeschwindigkeit des Kabels ab. Häufig wird dafür der NVP-Wert verwendet.

NVP

NVP steht für Nominal Velocity of Propagation und beschreibt die Signalausbreitung im Verhältnis zur Lichtgeschwindigkeit.

Ein falscher NVP-Wert führt zu einer falschen Entfernungsangabe.

Einordnung typischer Reflexionen

Beobachtung	mögliche Ursache
starke Reflexion am Leitungsende	offenes Ende oder Abschluss
starke Reflexion vor erwartetem Ende	Unterbrechung oder beschädigte Verbindung
Reflexion mit entgegengesetzter Charakteristik	Kurzschluss oder starke Impedanzänderung

Beobachtung	mögliche Ursache
mehrere Reflexionen	mehrere Steckstellen, Abzweigungen oder Beschädigungen
unplausible Entfernung	falscher NVP, falscher Kabeltyp oder komplexer Leitungsweg

“ Ein TDR lokalisiert eine elektrische Auffälligkeit. Es zeigt nicht automatisch, welches Bauteil dort tatsächlich beschädigt ist.

8. Tongenerator und Leitungssucher

Ein Tongenerator speist ein Suchsignal in eine Leitung ein. Ein Leitungssucher beziehungsweise eine induktive Prüfsonde hilft, dieses Signal an Kabeln, Patchfeldern oder Anschlussdosen zu erkennen.

Geeignet für:

- unbekannte Kabelwege,
- nicht dokumentierte Anschlussdosen,
- Zuordnung zwischen Dose und Patchfeld,
- Identifikation einzelner Leitungen in einem Bündel,
- grundlegende Durchgangsprüfung bei geeigneten Geräten.

Sichere Vorgehensweise

1. Leitung eindeutig bestimmen.
2. prüfen, ob sie aktiv ist oder Spannung führt.
3. Gerätespezifikation beachten.
4. Tongenerator passend anschließen.
5. Signal am vermuteten Leitungsweg verfolgen.
6. mehrere mögliche Leitungen vergleichen.
7. Leitung anschließend eindeutig beschriften.
8. Dokumentation aktualisieren.

Grenzen

- Nebensprechen kann das Signal auf benachbarte Kabel übertragen.
- ein starkes Signal beweist nicht immer die exakte Leitung.
- abgeschirmte Kabel können die Ortung beeinflussen.
- aktive Netzwerkverbindungen benötigen dafür geeignete Geräte.
- unbekannte elektrische Leitungen dürfen nicht ungeprüft angeschlossen werden.
- der Tongenerator bestätigt keine Ethernet-Leistungsfähigkeit.

9. Port- und Leitungslokalisierung über Link Blink

Einige Netzwerkprüfgeräte können den Link am Switchport gezielt auf- und abbauen oder ein Blinkmuster erzeugen.

Damit kann ein Administrator einen physischen Port identifizieren, ohne ausschließlich den Leitungsweg mit einem Tongenerator zu verfolgen.

Zu beachten

- Das Blinkmuster muss von einer zweiten Person oder Kamera am Switch beobachtet werden.
 - Ein produktiver Link kann dabei kurzzeitig unterbrochen werden.
 - Bei Link Aggregation, redundanten Pfaden oder Telefonen mit nachgeschaltetem PC können Nebenwirkungen entstehen.
 - Link Blink beweist lediglich die Zuordnung zum Port, nicht die Fehlerfreiheit des Kabels.
 - Switchport-Beschreibung, MAC-Tabelle und LLDP sollten zusätzlich geprüft werden.
-

10. Loopback-Stecker

Ein Loopback-Stecker führt Sende- und Empfangssignale an einer Schnittstelle kontrolliert zurück.

Mögliche Varianten existieren unter anderem für:

- Ethernet,
- serielle Schnittstellen,
- Glasfaser,
- USB,
- herstellerspezifische Diagnoseanschlüsse.

Mögliche Einsatzzwecke

- Schnittstelle lokal prüfen,
- Sende- und Empfangspfad testen,
- Diagnosefunktion eines Geräts ausführen,
- Port von Kabelweg und Gegenstelle trennen,
- Transceiver oder Adapter untersuchen.

Risiken

- Ein ungeeigneter Loopback-Stecker kann eine Schnittstelle beschädigen.
- Eine Netzwerkschleife kann entstehen.
- Spanning Tree kann reagieren.
- ein Port kann durch Schutzmechanismen deaktiviert werden.
- reflektierter Verkehr kann CPU- oder Netzlast erzeugen.
- optische Loopbacks müssen zum Fasertyp, Anschluss und Leistungsbereich passen.

Loopback-Stecker dürfen nur nach Herstelleranleitung und mit eindeutiger Zuordnung verwendet werden.

11. Vergleichshardware

Vergleichshardware hilft dabei, einen Fehler auf Gerät, Adapter, Kabel, Port oder Konfiguration einzugrenzen.

Geeignet sind beispielsweise:

- geprüfter USB-Netzwerkadapter,
- geprüfter USB-Hub,
- geprüfter SFP- oder SFP+-Transceiver,
- geprüfter Medienkonverter,
- geprüfter PoE-Injektor,
- geprüfter Access Point,
- geprüfter Switch,
- geprüfter Laptop,
- geprüftes Netzteil,
- geprüfter Konsolenadapter.

Kontrollierter Vergleich

1. nur eine Komponente verändern,
2. kompatible Vergleichshardware verwenden,
3. Versions- und Treiberunterschiede dokumentieren,
4. identische Verbindung erneut testen,
5. Ergebnis mit dem Ausgangszustand vergleichen,
6. ursprüngliche Komponente separat untersuchen.

Fehlinterpretationen vermeiden

Ergebnis	Einordnung
anderer Adapter funktioniert	ursprünglicher Adapter, Treiber oder dessen Kompatibilität ist verdächtig
anderer Laptop funktioniert	Fehler kann am ersten Client liegen, muss aber nicht ausschließlich Hardware sein
anderer Port funktioniert	ursprünglicher Port oder dessen Konfiguration ist verdächtig
anderer Transceiver funktioniert	ursprünglicher Transceiver oder dessen Kompatibilität ist verdächtig
Ersatznetzteil funktioniert	ursprüngliches Netzteil oder dessen Leistungsabgabe ist verdächtig

12. PoE-Tester

Ein PoE-Tester untersucht Power over Ethernet zwischen Power Sourcing Equipment und Powered Device.

Begriffe

Begriff	Bedeutung
PSE	stellt PoE-Leistung bereit, beispielsweise Switch oder Injektor
PD	empfängt PoE-Leistung, beispielsweise Access Point, Kamera oder Telefon
Endspan	PoE wird direkt durch den Switch bereitgestellt
Midspan	PoE wird durch einen zwischengeschalteten Injektor bereitgestellt
PoE-Klasse	handelt beziehungsweise beschreibt den Leistungsbedarf
PoE-Budget	insgesamt verfügbare Leistung eines Switches

Je nach Messgerät können untersucht werden:

- ob PoE vorhanden ist,
- verwendetes Adernpaar,
- Spannung,
- Klasse,
- angeforderte Leistung,
- verfügbare Leistung,
- Leistungsabgabe unter Last,
- Erkennung des PSE,
- Ethernet-Link,
- Switch- und VLAN-Informationen.

Typische PoE-Probleme

- PoE auf dem Port deaktiviert,
- Gesamtbudget des Switches erschöpft,
- falsche oder nicht unterstützte PoE-Klasse,
- hohe Leitungswiderstände,
- Widerstandsunsymmetrie,
- beschädigte Adernpaare,
- schlechte Auflegung,
- zu lange oder ungeeignete Verkabelung,
- inkompatibler passiver PoE-Injektor,
- nur bestimmte Ports unterstützen PoE,
- Gerät benötigt mehr Leistung als verfügbar,

- Leistung bricht erst unter Last zusammen,
- Port wurde durch Schutzmechanismus abgeschaltet.

PoE-Prüfreihenfolge

1. Leistungsanforderung des Endgeräts bestimmen.
2. unterstützten PoE-Standard des Switches prüfen.
3. PoE-Konfiguration und Gesamtbudget kontrollieren.
4. Messung direkt am Switchport durchführen.
5. Messung an der entfernten Netzwerkdose durchführen.
6. Spannungs- und Leistungsunterschied vergleichen.
7. Kabel auf Wiremap und Widerstandsprobleme prüfen.
8. Endgerät mit geprüfem Kabel und geeignetem PSE testen.
9. Ereignisprotokolle und Portstatus untersuchen.

“ Eine Leerlaufspannung bestätigt nicht, dass unter realer Last ausreichend Leistung zur Verfügung steht.

13. Passive PoE-Verbindungen

Passives PoE verwendet möglicherweise dauerhaft anliegende Spannung ohne standardisierte Aushandlung.

Risiken sind:

- Beschädigung nicht geeigneter Geräte,
- falsche Spannung,
- falsche Polarität,
- falsche Pinbelegung,
- Verwechslung mit standardisiertem IEEE-PoE,
- fehlende Schutzmechanismen.

Vor dem Anschließen müssen geprüft werden:

- Herstellerdokumentation,
- Spannung,
- Polarität,
- Pinbelegung,
- maximaler Strom,
- Kompatibilität des Endgeräts,
- Eignung des Messgeräts.

Passives PoE darf nicht allein anhand eines identischen RJ45-Steckers als kompatibel betrachtet werden.

14. Multimeter

Ein Multimeter kann abhängig von Gerät, Messleitungen und Qualifikation unter anderem messen:

- Spannung,
- Strom,
- Widerstand,
- Durchgang,
- teilweise Frequenz,
- teilweise Kapazität.

Mögliche IT-nahe Einsatzbereiche sind:

- Prüfung eines geeigneten Kleinspannungsnetzteils,
- Kontrolle dokumentierter Gleichspannungen,
- Durchgangsprüfung an spannungsfreien Leitungen,
- Untersuchung einer vorgesehenen Erdungs- oder Schirmverbindung,
- Vergleich einer gemessenen Ausgangsspannung mit der Herstellerangabe.

Gefahren

- falscher Messbereich,
- Messleitung in falscher Buchse,
- Strommessung parallel zur Spannungsquelle,
- Messung an Netzspannung ohne Qualifikation,
- ungeeignete Messkategorie,
- beschädigte Messleitungen,
- Kurzschluss durch Prüfspitzen,
- Messung an unbekannten Stromkreisen,
- unzulässige Öffnung von Geräten oder Netzteilen.

Verbindliche Begrenzung

Multimeter dürfen nur durch dafür qualifizierte Personen, mit geeignetem Messgerät und innerhalb des zulässigen Einsatzbereichs verwendet werden.

“ Ein IT-Administrator sollte keine Arbeiten an Netzspannung, Stromverteilungen oder geöffneten Netzteilen durchführen, wenn dafür die elektrotechnische Qualifikation und Freigabe fehlen.

15. Netzteil- und Stromversorgungsprüfung

Viele scheinbare Netzwerk- oder Gerätefehler entstehen durch die Stromversorgung.

Zu prüfen sind:

- sitzt der Netzstecker vollständig?
- ist die Steckdosenleiste eingeschaltet?
- zeigt die USV einen Alarm?
- ist das richtige Netzteil angeschlossen?
- stimmen Ausgangsspannung, Strombelastbarkeit und Polarität?
- ist das Netzteil ungewöhnlich warm?
- treten Neustarts nur unter Last auf?
- funktionieren redundante Netzteile?
- sind beide Netzteile tatsächlich an getrennte Strompfade angeschlossen?
- bestehen Ereignisse zu Unterspannung oder Stromverlust?
- ist der PoE-Port ausreichend dimensioniert?
- sind Sicherungen oder Schutzschalter ausgelöst?

Typische Fehlerbilder

Beobachtung	mögliche Ursache
Gerät startet wiederholt neu	instabiles Netzteil, Überlast, Temperatur oder Hardwarefehler
Gerät funktioniert ohne Zusatzmodule	Netzteil zu schwach oder defektes Modul
redundante Netzteile angezeigt, aber nur ein Stromkreis	keine vollständige Stromredundanz
Fehler nur bei hoher Last	Spannungseinbruch, Leistungsgrenze oder Kühlungsproblem
USV meldet Batteriebetrieb	Stromversorgung vor der USV oder Netzqualität prüfen
Gerät bleibt nach Stromausfall aus	Startverhalten, Netzteil, USV oder Hardwarezustand

16. Glasfaser-Grundlagen für die Messung

Vor einer Glasfasermessung müssen bekannt sein:

- Singlemode oder Multimode,
- Faserkategorie,
- Wellenlänge,
- Steckertyp,
- Schliffart,
- Sendeleistung,
- zulässiger Empfangsbereich,
- Linkbudget,

- Anzahl der Steckverbindungen,
- Anzahl der Spleiße,
- Streckenlänge,
- erwartete Dämpfung,
- verwendete Transceiver.

Häufige Steckertypen

- LC,
- SC,
- ST,
- MPO beziehungsweise MTP.

Wichtige Unterscheidungen

- Singlemode und Multimode dürfen nicht beliebig kombiniert werden.
- UPC- und APC-Schliffe dürfen nicht direkt miteinander verbunden werden.
- unterschiedliche Wellenlängen führen zu unterschiedlichen Messwerten.
- optische Pegel werden häufig in dBm angegeben.
- Verlust beziehungsweise Dämpfung wird häufig in dB angegeben.

dBm und dB

Einheit	Bedeutung
dBm	absoluter optischer Leistungspegel bezogen auf 1 mW
dB	Verhältnis beziehungsweise Verlust zwischen zwei Pegeln

“ Ein Wert von **-10 dBm** ist kein Verlust von **-10 dB**. Absoluter Pegel und Streckendämpfung müssen getrennt behandelt werden.

17. Glasfaser inspizieren und reinigen

Verschmutzte Steckerendflächen gehören zu den häufigsten Ursachen optischer Probleme.

Mögliche Verunreinigungen sind:

- Staub,
- Hautfett,
- Reinigungsrückstände,
- Abrieb,
- Feuchtigkeit,
- Schmutz aus Schutzkappen.

Grundregel

inspizieren

→ bei Bedarf reinigen

→ erneut inspizieren

→ erst danach verbinden

Benötigte Werkzeuge können sein:

- geeignetes Glasfaser-Inspektionsmikroskop,
- Videosonde,
- passende Adapterspitzen,
- fusselfreie Reinigungstücher,
- geeignete Reinigungsflüssigkeit,
- One-Click-Reiniger,
- Reinigungswerkzeuge für MPO/MTP,
- saubere Schutzkappen.

Wichtige Regeln

- niemals in eine aktive Glasfaser blicken,
- vor der Inspektion Aktivität beziehungsweise Laserquelle sicher berücksichtigen,
- keine ungeeigneten Haushaltsreiniger verwenden,
- Stecker nicht mit Kleidung oder Fingern reinigen,
- gereinigte Endflächen nicht berühren,
- auch werksseitig konfektionierte Stecker vor dem Verbinden prüfen,
- Adapter und Messleitungen ebenfalls kontrollieren,
- verschmutzte Schutzkappen nicht wiederverwenden.

“ Eine verschmutzte Endfläche kann nicht nur die Messung verfälschen, sondern beim Verbinden auch die Gegenseite verschmutzen oder beschädigen.

18. Visual Fault Locator

Ein Visual Fault Locator speist sichtbares rotes Licht in eine Glasfaser ein.

Er kann helfen bei:

- Identifikation einer Faser,
- Polaritätsprüfung,
- Erkennung grober Unterbrechungen,
- Auffinden starker Biegungen,

- Erkennung schlechter Steckverbindungen,
- Untersuchung kurzer Leitungsabschnitte.

Grenzen

- nicht jede Beschädigung wird sichtbar,
- lange Strecken können das sichtbare Licht stark dämpfen,
- Kabelummantelung kann austretendes Licht verdecken,
- ein sichtbarer Lichtaustritt lokalisiert nicht automatisch die genaue Fehlerursache,
- ein VFL ersetzt keine Dämpfungsmessung,
- ein VFL ersetzt kein OTDR,
- Laserklassifizierung und Sicherheitsregeln müssen beachtet werden.

19. Optischer Leistungsmesser

Ein optischer Leistungsmesser misst den empfangenen optischen Pegel.

Vor der Messung müssen bekannt sein:

- Wellenlänge,
- zulässiger Empfangsbereich,
- verwendeter Anschlussadapter,
- erwarteter Sendepiegel,
- Empfindlichkeit und Übersteuerungsgrenze des Empfängers,
- Referenzwert,
- Fasertyp.

Mögliche Ergebnisse

Messwert	Einordnung
innerhalb des zulässigen Bereichs	Pegel ist grundsätzlich geeignet
unterhalb der Empfindlichkeitsgrenze	Signal zu schwach
oberhalb der Übersteuerungsgrenze	Signal zu stark
stark schwankender Pegel	instabile Quelle, Stecker, Faser oder Bewegung
kein Pegel	falsche Faser, Sender aus, Unterbrechung oder falsche Wellenlänge
Pegel ausreichend, Link bleibt down	Ursache kann Transceiver, Protokoll, Geschwindigkeit oder Gegenstelle sein

Typische Ursachen für zu geringe Leistung

- verschmutzte Endfläche,
- beschädigtes Patchkabel,
- zu viele Steckverbindungen,

- ungeeigneter Spleiß,
 - Makro- oder Mikrobiegung,
 - falsche Faser,
 - falscher Transceiver,
 - zu große Streckenlänge,
 - schwache Sendeleistung,
 - ungeeignete Wellenlänge.
-

20. Optical Loss Test Set

Ein Optical Loss Test Set besteht typischerweise aus Lichtquelle und Leistungsmesser. Es bestimmt die Einfügedämpfung einer Glasfaserstrecke.

Vereinfachtes Verfahren

Referenzmessung

- Messleitungen und Lichtquelle referenzieren
- zu prüfende Strecke einfügen
- empfangenen Pegel messen
- Verlust bestimmen
- mit Grenzwert vergleichen

Vorher festzulegen sind:

- Fasertyp,
- Wellenlänge,
- Referenzmethode,
- Anzahl der Test-Referenzkabel,
- Steckertyp,
- Messrichtung,
- Grenzwert,
- erwartete Linkdämpfung.

Fehlerquellen bei der Messung

- verschmutzte Referenzkabel,
- beschädigte Messadapter,
- falsche Referenzmethode,
- Bewegung der Testleitungen,
- falsche Wellenlänge,
- unterschiedliche Steckerschlitze,
- nicht stabilisierte Lichtquelle,
- falscher Nullabgleich,
- vertauschte Polarität,

- unterschiedliche Messaufbauten.

“ Eine Messung ist nur dann vergleichbar, wenn Referenzmethode, Wellenlänge, Messleitungen und Grenzwerte dokumentiert wurden.

21. OTDR für Glasfaser

Ein Optical Time Domain Reflectometer sendet optische Impulse in eine Faser und wertet das zurückgestreute beziehungsweise reflektierte Licht über die Zeit aus.

Ein OTDR kann je nach Gerät darstellen:

- Faserlänge,
- Steckverbindungen,
- Spleiße,
- Reflexionsereignisse,
- nicht reflektierende Ereignisse,
- Dämpfung einzelner Abschnitte,
- Gesamtdämpfung,
- Unterbrechung,
- ungefähre Entfernung zur Fehlerstelle.

Vereinfachte Darstellung

OTDR

→ optischer Impuls

→ Rückstreuung entlang der Faser

→ Reflexionen an Ereignissen

→ Ereignistabelle und Kurve

Launch- und Receive-Faser

Eine Vorlauffaser kann erforderlich sein, um:

- den ersten Anschluss außerhalb der Totzone zu messen,
- den Eingangsstecker zu beurteilen,
- einen realistischen Leitungsanfang darzustellen.

Eine Nachlauffaser kann erforderlich sein, um:

- den letzten Anschluss zu beurteilen,
- das Ende der Strecke korrekt auszuwerten.

Wichtige OTDR-Einstellungen

- Wellenlänge,
- Messbereich,
- Pulsbreite,
- Messdauer,
- Brechungsindex,
- Rückstreukoeffizient,
- Ereignisschwelle,
- Fasertyp.

Einfluss der Pulsbreite

Einstellung	Vorteil	Nachteil
kurze Pulsbreite	bessere Auflösung nahe beieinanderliegender Ereignisse	geringere Reichweite und schwächeres Signal
lange Pulsbreite	größere Reichweite und besserer Dynamikbereich	größere Totzonen und geringere Ereignisauflösung

Grenzen

- nahe Ereignisse können in einer Totzone liegen,
- Reflexionen können Geisterereignisse erzeugen,
- falsche Einstellungen führen zu falscher Entfernung oder Dämpfung,
- bidirektionale Messungen können für belastbare Bewertung erforderlich sein,
- ein OTDR ersetzt nicht automatisch eine normgerechte Einfügedämpfungsmessung,
- Bedienung und Kurveninterpretation erfordern Fachkenntnisse.

22. SFP- und Transceiver-Diagnose

Viele Transceiver unterstützen Digital Optical Monitoring beziehungsweise Digital Diagnostic Monitoring.

Mögliche Werte sind:

- Temperatur,
- Versorgungsspannung,
- Sendeleistung,
- Empfangsleistung,
- Laser-Bias-Strom,
- Warn- und Alarmgrenzen.

Beispielhafte Einordnung

Beobachtung	mögliche Ursache
-------------	------------------

Empfangsleistung zu niedrig	Dämpfung, Verschmutzung, falsche Faser oder schwacher Sender
Empfangsleistung zu hoch	ungeeigneter Transceiver oder fehlendes Dämpfungsglied
Sendeleistung außerhalb der Grenze	Transceiverfehler oder Temperaturproblem
hohe Temperatur	unzureichende Kühlung, hoher Umgebungswert oder Modulproblem
Werte nur auf einer Seite auffällig	Richtung der Faserstrecke gezielt untersuchen
keine Diagnosedaten	Modul unterstützt DDM nicht oder Gerät liest es nicht aus

Zusätzlich prüfen

- unterstützter Transceivertyp,
- Herstellerkompatibilität,
- Geschwindigkeit,
- Wellenlänge,
- Singlemode oder Multimode,
- Duplex- oder BiDi-Verfahren,
- Faserpolarität,
- Steckertyp,
- Gegenstellenmodul,
- Fehlerzähler,
- Forward Error Correction,
- verwendete Breakout-Konfiguration.

“ Optische Diagnosedaten des Transceivers sind hilfreich, ersetzen aber keine unabhängige Messung bei unklaren oder widersprüchlichen Ergebnissen.

23. WLAN-Spektrumanalysator

Ein WLAN-Scanner zeigt hauptsächlich WLAN-Netze und deren Protokollinformationen. Ein Spektrumanalysator untersucht dagegen die Hochfrequenzenergie im verwendeten Frequenzbereich und kann auch nicht WLAN-basierte Störquellen sichtbar machen.

Mögliche Untersuchungen

- Kanalbelegung,
- Kanalnutzung,
- Störpegel,
- dauerhafte oder periodische Signale,
- Interferenzen,
- überlappende Kanäle,
- nicht WLAN-basierte Sender,

- zeitlicher Verlauf,
- Nutzung der Frequenzbänder 2,4 GHz, 5 GHz oder 6 GHz abhängig vom Gerät.

Mögliche Störquellen

- andere WLAN-Netze,
- Bluetooth,
- Funkkameras,
- drahtlose Videoübertragung,
- Mikrowellengeräte,
- fehlerhafte elektrische Geräte,
- bestimmte Sensoren,
- Radarerkennung im 5-GHz-Bereich,
- breitbandige Störsender.

Messparameter

- Frequenz,
- Kanal,
- Signalstärke,
- Rauschpegel,
- Kanalnutzung,
- Duty Cycle,
- zeitliches Auftreten,
- Signalbreite,
- räumliche Veränderung.

Vorgehensweise

1. betroffenen Ort bestimmen.
2. Zeitpunkt und Symptom dokumentieren.
3. Messung am betroffenen Clientstandort durchführen.
4. Vergleichsmessung an einem funktionierenden Standort durchführen.
5. zeitlichen Verlauf beobachten.
6. Störquelle durch räumliche Messungen eingrenzen.
7. WLAN-Konfiguration und Spektrummessung gemeinsam auswerten.
8. Änderung kontrolliert testen.
9. erneut messen.

“ Eine hohe WLAN-Signalstärke bestätigt keine geringe Interferenz und keine gute Signalqualität.

24. WLAN-Site-Survey-Werkzeuge

Ein Site Survey untersucht die räumliche WLAN-Versorgung.

Mögliche Ergebnisse sind:

- Signalstärke,
- Signal-Rausch-Abstand,
- Kanalnutzung,
- Access-Point-Zuordnung,
- Datenrate,
- Überlappung,
- Roamingbereiche,
- Störquellen,
- erwartete Abdeckung,
- tatsächliche Abdeckung.

Arten

Art	Beschreibung
Predictive Survey	rechnerische Planung anhand von Gebäude- und Materialdaten
Passive Survey	Empfang und Auswertung vorhandener Funksignale
Active Survey	aktive Verbindung und Messung von Netzwerkleistung
Spectrum Survey	Untersuchung der Funkenergie einschließlich nicht WLAN-basierter Quellen

Zu beachten

- Grundriss und Maßstab müssen stimmen.
- Wandmaterialien beeinflussen das Ergebnis.
- Möbel, Personen und Türen verändern Funkbedingungen.
- Messgerät und Antennenausrichtung beeinflussen Messwerte.
- verschiedene Clienttypen besitzen unterschiedliche Funkfähigkeiten.
- eine leere Umgebung kann andere Ergebnisse liefern als der spätere Produktivbetrieb.
- Messungen müssen für relevante Frequenzbänder getrennt betrachtet werden.

25. Temperaturmessung und Wärmebildkamera

Temperaturprobleme können zu instabilen Geräten, Leistungseinbrüchen und vorzeitigem Hardwareausfall führen.

Mögliche Werkzeuge sind:

- interne Temperatursensoren,
- Kontaktthermometer,

- Infrarotthermometer,
- Wärmebildkamera,
- Umgebungssensoren,
- Sensoren im Rack oder Rechenzentrum.

Zu prüfen sind

- Lufteinlass- und Auslasstemperatur,
- blockierte Lüftungswege,
- ausgefallene Lüfter,
- falsche Luftstromrichtung,
- Hotspots,
- ungewöhnlich warme Netzteile,
- überhitzte Transceiver,
- Rackposition,
- Umgebungstemperatur,
- Staubbelastung,
- Veränderungen unter Last.

Grenzen von Infrarotmessungen

- reflektierende Oberflächen können Messwerte verfälschen,
 - Emissionsgrad beeinflusst das Ergebnis,
 - Entfernung und Messfleckgröße müssen berücksichtigt werden,
 - eine Oberflächentemperatur entspricht nicht automatisch der internen Bauteiltemperatur,
 - Vergleichswerte sollten unter ähnlichen Bedingungen erhoben werden.
-

26. Serielle Konsole

Eine serielle Konsole ermöglicht lokalen Zugriff, wenn das normale Managementnetz nicht funktioniert.

Mögliche Anschlüsse sind:

- RJ45-Konsole,
- USB-Konsole,
- USB-C-Konsole,
- RS-232,
- herstellerspezifische Konsolenschnittstelle.

Benötigt werden gegebenenfalls:

- passendes Konsolenkabel,
- USB-Seriell-Adapter,
- geeigneter Treiber,
- Terminalprogramm,

- korrekte Übertragungsparameter.

Typische Parameter

Geschwindigkeit: 9600 oder herstellerspezifisch

Datenbits: 8

Parität: keine

Stoppbits: 1

Flusssteuerung: keine

Die konkreten Werte müssen der Herstellerdokumentation entnommen werden.

Mögliche Diagnoseinformationen

- Bootmeldungen,
- Hardwarefehler,
- Dateisystemfehler,
- fehlgeschlagene Module,
- Konfigurationsprobleme,
- Management-IP,
- Recovery-Menü,
- Firmwarestatus.

Sicherheitsregeln

- Konsolenzugriff ist privilegierter Zugriff.
- Konsolenkabel und Terminalserver müssen geschützt werden.
- Bootmeldungen können vertrauliche Informationen enthalten.
- Kennwortwiederherstellung kann Konfiguration oder Verfügbarkeit beeinflussen.
- Recovery-Verfahren dürfen nur mit Freigabe durchgeführt werden.

27. Out-of-Band-Management

Out-of-Band-Management verwendet einen vom normalen Datenpfad getrennten Managementweg.

Beispiele sind:

- Konsolenserver,
- dediziertes Managementnetz,
- Mobilfunkverbindung für Notfallzugriff,
- HPE iLO,
- Dell iDRAC,
- IPMI-basierte Managementcontroller,
- Cisco CIMC,

- KVM over IP.

Mögliche Funktionen

- Hardwarezustand anzeigen,
- Sensoren und Ereignisprotokolle prüfen,
- Remote-Konsole öffnen,
- Startvorgang beobachten,
- Gerät kontrolliert ein- oder ausschalten,
- virtuelle Medien bereitstellen,
- Firmware verwalten,
- ausgefallenes Betriebssystem unabhängig untersuchen.

Sicherheitsanforderungen

- getrenntes Managementnetz,
- Zugriff nur für berechtigte Administratoren,
- Multifaktor-Authentifizierung, sofern unterstützt,
- aktuelle Firmware,
- keine direkte öffentliche Erreichbarkeit,
- sichere Protokolle,
- zentrale Protokollierung,
- individuelle Konten,
- eingeschränkte Firewallregeln,
- Notfallzugriff dokumentieren und testen,
- Standardkennwörter entfernen,
- Zertifikate prüfen.

“ Out-of-Band-Management ist kein gewöhnliches Messgerät, aber ein unabhängiger Diagnoseweg zur physischen Hardware und zum Startvorgang.

28. In-Band und Out-of-Band unterscheiden

Merkmal	In-Band-Management	Out-of-Band-Management
Datenpfad	nutzt reguläres Netzwerk	nutzt separaten Managementweg
Abhängigkeit vom Betriebssystem	häufig vorhanden	häufig geringer oder keine
Zugriff bei Routingfehler	möglicherweise nicht möglich	bei funktionsfähigem OOB-Pfad weiterhin möglich
Zugriff während des Bootens	meist eingeschränkt	häufig möglich
Risiko	Ausfall des Produktivnetzes blockiert Zugriff	separater Weg muss besonders geschützt werden

Merkmal	In-Band-Management	Out-of-Band-Management
Beispiele	SSH, HTTPS, SNMP	Konsole, iLO, iDRAC, CIMC, IPMI, Konsolenserver

Eine physisch vorhandene Managementbuchse bestätigt nicht automatisch, dass ein vollständig unabhängiger Out-of-Band-Pfad aufgebaut wurde.

29. Messgerät selbst überprüfen

Auch ein Messgerät kann fehlerhaft sein.

Vor wichtigen Messungen prüfen:

- Akkustand,
- Netzteil,
- Firmwarestand,
- Selbsttest,
- Kalibrierungsdatum,
- Messadapter,
- Messleitungen,
- Steckverbinder,
- Referenzkabel,
- richtige Geräteeinstellung,
- richtige Wellenlänge,
- richtiger Kabeltyp,
- richtiger Grenzwert,
- Datum und Uhrzeit,
- Speicherplatz,
- gespeicherte Kunden- oder Projektdaten.

Kontrollmessung

Eine Kontrollmessung an einer bekannten, funktionierenden Referenz hilft dabei, Fehler des Messaufbaus zu erkennen.

“ Wenn ein unerwartetes Ergebnis große Folgen hätte, sollte es mit einer zweiten Messung, einem anderen Messaufbau oder einem unabhängigen Messgerät bestätigt werden.

30. Kalibrierung und Rückführbarkeit

Bei Zertifizierungs- und Abnahmemessungen ist die Kalibrierung besonders wichtig.

Zu dokumentieren sind:

- Hersteller und Modell,
- Seriennummer,
- Firmwareversion,
- Kalibrierungsdatum,
- nächster Kalibrierungstermin,
- verwendete Adapter,
- verwendete Referenzleitungen,
- Prüfstandard,
- Messperson,
- Datum und Uhrzeit,
- Messort.

Eine abgelaufene Kalibrierung bedeutet nicht zwangsläufig, dass jeder Messwert falsch ist. Sie kann jedoch die Nachweisbarkeit und Verwendbarkeit der Messergebnisse beeinträchtigen.

31. Messergebnisse dokumentieren

Eine Messung sollte mindestens folgende Angaben enthalten:

Feld	Inhalt
Ticket oder Vorgang	eindeutige Referenz
Datum und Uhrzeit	Zeitpunkt der Messung
Messperson	verantwortliche Person
Standort	Gebäude, Raum, Rack oder Anschluss
Verbindung	Start- und Endpunkt
Gerät	Hersteller, Modell und Seriennummer
Messgerät	Hersteller, Modell und Seriennummer
Kalibrierung	gültig bis beziehungsweise Status
Messaufbau	Permanent Link, Channel, direkt am Port oder anderer Aufbau
Einstellung	Standard, Wellenlänge, NVP, Pulsbreite oder Messbereich
Ausgangszustand	ursprüngliches Symptom
Messwert	tatsächliches Ergebnis
Grenzwert	erwarteter beziehungsweise zulässiger Wert
Maßnahme	kontrollierte Änderung
Nachmessung	Ergebnis nach der Maßnahme
Anhänge	Fotos, Kurven, Berichte oder Exportdateien

Beispiel

Verbindung: Patchfeld A-17 → Datendose B-204

Symptom: Link fällt mehrmals pro Stunde auf 100 Mbit/s zurück

Messgerät: Kabelzertifizierer, Seriennummer dokumentiert

Messaufbau: Permanent Link

Grenzwert: Cat 6A

Ergebnis: nicht bestanden

Auffälligkeit: NEXT am nahen Anschluss

Fehlerentfernung: innerhalb des Anschlussbereichs

Maßnahme: Anschluss neu aufgelegt

Nachmessung: bestanden

Funktionstest: stabiler 1-Gbit/s-Link, Fehlerzähler steigen nicht weiter

32. Messwerte richtig vergleichen

Vergleichsmessungen sind nur sinnvoll, wenn die Bedingungen vergleichbar sind.

Zu berücksichtigen sind:

- identischer Messpunkt,
- identisches Messgerät,
- identische Adapter,
- identische Geräteeinstellung,
- identische Wellenlänge,
- identischer Kabeltyp,
- gleiche Messrichtung,
- ähnliche Temperatur,
- gleicher Betriebszustand,
- gleiche Last,
- gleicher Zeitraum,
- gleiche Referenzmethode.

Ungültige Vergleiche

- dBm und dB direkt gleichsetzen,
 - OTDR-Dämpfung ohne Kontext mit OLTS-Messung vergleichen,
 - Permanent-Link-Messung mit Channel-Messung gleichsetzen,
 - PoE-Leerlaufwert mit Leistung unter Last gleichsetzen,
 - WLAN-Messungen an verschiedenen Standorten ohne Positionsangabe vergleichen,
 - Messwerte verschiedener Wellenlängen gleichsetzen,
 - Kabellängen mit falschem NVP vergleichen.
-

33. Kontrollierte Prüfreihefolge bei Kupferproblemen

1. Symptom und betroffene Verbindung bestimmen.
 2. Portstatus und Fehlerzähler dokumentieren.
 3. sichtbare Schäden prüfen.
 4. Steckverbindungen kontrollieren.
 5. geprüfetes Patchkabel verwenden.
 6. Gegenstelle mit Vergleichshardware testen.
 7. Wiremap und Kabellänge prüfen.
 8. Fehlerentfernung mit TDR untersuchen.
 9. bei Leistungsanforderungen qualifizieren oder zertifizieren.
 10. PoE gegebenenfalls unter Last messen.
 11. Anschlussstellen und Patchfeld untersuchen.
 12. nach jeder Maßnahme erneut messen.
 13. Konfiguration und physische Messung gemeinsam bewerten.
 14. Ursache und Ergebnis dokumentieren.
-

34. Kontrollierte Prüfreihefolge bei Glasfaserproblemen

1. Fasertyp, Wellenlänge und Transceiver bestimmen.
 2. Portstatus und optische Diagnosedaten dokumentieren.
 3. richtige Polarität prüfen.
 4. Endflächen sicher inspizieren.
 5. bei Bedarf reinigen und erneut inspizieren.
 6. geprüfetes Patchkabel einsetzen.
 7. sichtbare Fehlersuche nur mit geeignetem VFL durchführen.
 8. optischen Empfangspegel messen.
 9. Streckendämpfung mit geeigneter Lichtquelle und Leistungsmesser bestimmen.
 10. Ereignisse und Fehlerentfernung bei Bedarf mit OTDR untersuchen.
 11. Messung gegebenenfalls in Gegenrichtung wiederholen.
 12. Ergebnis mit Linkbudget und Grenzwerten vergleichen.
 13. nach jeder Maßnahme erneut messen.
 14. Messkurven und Berichte sichern.
-

35. Praxisbeispiel: Link fällt auf 100 Mbit/s zurück

Symptom

Ein Gigabit-Endgerät verbindet sich nur mit 100 Mbit/s oder wechselt wiederholt zwischen Geschwindigkeiten.

Prüfung

1. unterstützte Geschwindigkeiten beider Geräte prüfen.
2. Auto-Negotiation auf beiden Seiten kontrollieren.

3. Portstatus und Fehlerzähler dokumentieren.
4. geprüfetes Patchkabel einsetzen.
5. alle vier Adernpaare mit Kabeltester prüfen.
6. feste Gebäudeverkabelung untersuchen.
7. Split Pair, Unterbrechung oder schlechte Auflegung prüfen.
8. Verbindung bei Bedarf qualifizieren oder zertifizieren.
9. Vergleichsport und Vergleichsadapter verwenden.
10. nach der Maßnahme Linkgeschwindigkeit und Fehlerzähler erneut prüfen.

Mögliche Ursachen

- ein Adernpaar unterbrochen,
 - schlechte Auflegung,
 - ungeeignetes Patchkabel,
 - beschädigte Dose,
 - fehlerhafter Port,
 - defekter Netzwerkadapter,
 - falsche Konfiguration,
 - unzureichende Signalqualität.
-

36. Praxisbeispiel: PoE-Gerät startet wiederholt neu

Symptom

Ein Access Point oder eine Kamera startet unter Last neu.

Prüfung

1. PoE-Anforderung des Geräts bestimmen.
2. unterstützten Standard und Port des Switches prüfen.
3. verfügbares Gesamtbudget kontrollieren.
4. Switchprotokolle untersuchen.
5. Leistung direkt am Switchport prüfen.
6. Leistung an der entfernten Dose unter Last prüfen.
7. Kabelweg und Widerstandsunsymmetrie untersuchen.
8. geprüfetes kurzes Kabel verwenden.
9. geeigneten Vergleichsport oder PSE einsetzen.
10. Temperatur und Firmware berücksichtigen.

Mögliche Ursachen

- Leistungsbudget erschöpft,
- falsche PoE-Klasse,
- hoher Spannungsabfall,
- beschädigtes Adernpaar,
- schlechte Auflegung,

- ungeeigneter Injektor,
 - defektes Endgerät,
 - Überhitzung,
 - fehlerhafte Switchkonfiguration.
-

37. Praxisbeispiel: Glasfaserlink bleibt down

Prüfung

1. Transceivertypen auf beiden Seiten vergleichen.
2. Geschwindigkeit und Wellenlänge prüfen.
3. Singlemode beziehungsweise Multimode prüfen.
4. Faserpolarität kontrollieren.
5. Transceiver vollständig einsetzen.
6. optische Diagnosedaten auslesen.
7. Endflächen inspizieren und fachgerecht reinigen.
8. geprüfetes Patchkabel verwenden.
9. optischen Pegel messen.
10. Strecke mit OLTS beziehungsweise OTDR untersuchen.
11. Transceiver kontrolliert austauschen.
12. Port- und Gerätekonfiguration prüfen.

Mögliche Ursachen

- vertauschte Sende- und Empfangsfaser,
 - falscher Transceiver,
 - inkompatible Wellenlänge,
 - verschmutzte Endfläche,
 - beschädigtes Patchkabel,
 - zu hohe Dämpfung,
 - Unterbrechung,
 - Port administrativ deaktiviert,
 - unterschiedliche Geschwindigkeit,
 - fehlerhafter Transceiver.
-

38. Praxisbeispiel: WLAN ist nur in einem Raum instabil

Prüfung

1. betroffene Clients und Zeiten bestimmen.
2. Signalstärke und SNR messen.
3. Kanal und Kanalnutzung prüfen.
4. Spektrum am betroffenen Ort untersuchen.
5. Vergleichsmessung außerhalb des Raums durchführen.
6. zeitabhängige Störquelle suchen.

7. Wandmaterialien und Raumaufteilung berücksichtigen.
8. Client mit Vergleichshardware testen.
9. Access-Point-Position und Sendeleistung prüfen.
10. Änderung nur einzeln durchführen und erneut messen.

Mögliche Ursachen

- nicht WLAN-basierte Störquelle,
- starke Kanalüberlagerung,
- ungünstige Abschirmung,
- Metallflächen,
- fehlerhafter Clientadapter,
- zu hohe oder zu niedrige Sendeleistung,
- ungeeignete Kanalbreite,
- Roamingproblem,
- hohe Kanalnutzung.

39. Praxisbeispiel: Server ist über das Netzwerk nicht erreichbar

Prüfung

1. Stromversorgung und Statusanzeigen prüfen.
2. Switchport und Kabel untersuchen.
3. Out-of-Band-Management testen.
4. Hardwareereignisse und Sensoren prüfen.
5. Remote-Konsole öffnen.
6. Bootstatus beobachten.
7. Betriebssystem- und Netzwerkzustand prüfen.
8. bei Bedarf geprüftes Kabel und Vergleichsport verwenden.
9. Netzteil- und Temperaturzustand untersuchen.
10. Neustart nur nach Freigabe und Beweissicherung durchführen.

Mögliche Ergebnisse

Ergebnis	Einordnung
Out-of-Band erreichbar, Betriebssystem nicht	Betriebssystem, Treiber, Netzwerkdienst oder Konfiguration
weder In-Band noch Out-of-Band erreichbar	Stromversorgung, Managementpfad oder Hardware
Remote-Konsole zeigt Startfehler	Bootmedium, Dateisystem, Firmware oder Hardware
Hardwarestatus zeigt Alarm	betroffene Komponente gezielt untersuchen
anderer Switchport funktioniert	ursprünglicher Port oder dessen Konfiguration
geprüftes Kabel funktioniert	ursprüngliche Verkabelung verdächtig

40. Häufige Fehlinterpretationen

Aussage	fachliche Einordnung
„Der Kabeltester zeigt alle Adern, also ist das Kabel für 10 Gbit/s geeignet.“	Ein einfacher Wiremap-Test zertifiziert keine Übertragungsleistung.
„Mit dem Ersatzkabel funktioniert es, also ist sicher nur das Kabel defekt.“	Auch ein Steckkontakt oder eine veränderte mechanische Belastung kann beteiligt sein.
„PoE-Spannung ist vorhanden, also reicht die Leistung aus.“	Entscheidend ist die verfügbare Leistung unter Last.
„Der optische Pegel ist sichtbar, also ist die Faser in Ordnung.“	Pegel, Dämpfung, Reflexionen, Polarität und Protokoll müssen getrennt geprüft werden.
„Das OTDR zeigt einen Fehler bei 20 Metern, also ist dort sicher das Kabel gebrochen.“	Die Anzeige beschreibt ein optisches Ereignis; Messparameter und Leitungsweg müssen berücksichtigt werden.
„Starke WLAN-Signalstärke bedeutet eine gute Verbindung.“	Interferenz, SNR, Kanalnutzung und Retries können die Verbindung trotzdem beeinträchtigen.
„Die Temperatur fühlt sich normal an.“	subjektive Wahrnehmung ersetzt keine Messung und keine Herstellergrenze.
„Der Managementport ist erreichbar, also ist der Server vollständig in Ordnung.“	Out-of-Band-Zugriff bestätigt nicht den Zustand des Betriebssystems oder der Anwendung.
„Ein Multimeter ist ungefährlich, weil nur Kleinspannung gemessen wird.“	falsche Bedienung und unbekannte Stromkreise können weiterhin Schäden verursachen.
„Ein einmal bestandener Test beweist dauerhaft fehlerfreie Verkabelung.“	Kabel, Stecker und Umgebungsbedingungen können sich später verändern.

41. Checkliste physische Messgeräte

- ☐ betroffene Verbindung und deren Funktion sind bekannt.
- ☐ Wartungs- oder Änderungsfreigabe wurde geprüft.
- ☐ Ausgangszustand wurde dokumentiert.
- ☐ Kabel und Anschlüsse wurden eindeutig beschriftet.
- ☐ Sichtprüfung wurde durchgeführt.
- ☐ geeignetes Messgerät wurde ausgewählt.
- ☐ Messgerät und Adapter sind unbeschädigt.
- ☐ Kalibrierungsstatus wurde geprüft.
- ☐ richtige Messleitungen wurden verwendet.
- ☐ richtige Geräteeinstellung wurde gewählt.
- ☐ Referenzwert und Grenzwert sind bekannt.
- ☐ geprüftes Ersatzkabel ist verfügbar.

- ☐ immer nur eine Komponente wurde verändert.
- ☐ Kupfermessung unterscheidet Verification, Qualification und Certification.
- ☐ TDR-Messung verwendet einen passenden NVP-Wert.
- ☐ PoE wurde bei Bedarf unter Last geprüft.
- ☐ passive PoE-Verbindungen wurden nicht ungeprüft angeschlossen.
- ☐ Multimeter wurde nur durch qualifizierte Personen eingesetzt.
- ☐ Glasfasertyp und Wellenlänge wurden bestimmt.
- ☐ aktive Glasfaser wurde sicher behandelt.
- ☐ Glasfaser wurde inspiziert, gereinigt und erneut inspiziert.
- ☐ optischer Pegel und Streckendämpfung wurden unterschieden.
- ☐ OTDR-Einstellungen und Totzonen wurden berücksichtigt.
- ☐ Launch- und Receive-Faser wurden bei Bedarf verwendet.
- ☐ WLAN-Scanner und Spektrumanalysator wurden unterschieden.
- ☐ Vergleichsmessung wurde unter vergleichbaren Bedingungen durchgeführt.
- ☐ Out-of-Band-Zugriff wurde sicher verwendet.
- ☐ Messwerte, Einstellungen und Messpunkte wurden dokumentiert.
- ☐ Nachmessung nach der Maßnahme wurde durchgeführt.
- ☐ Funktion und mögliche Nebenwirkungen wurden geprüft.
- ☐ Messberichte wurden sicher gespeichert.

42. Schnellreferenz

Werkzeug	Hauptzweck	bestätigt nicht automatisch
geprüftes Ersatzkabel	verdächtiges Kabel kontrolliert vergleichen	Fehlerfreiheit der festen Verkabelung
einfacher Kabeltester	Wiremap, Unterbrechung und Kurzschluss prüfen	Einhaltung einer Kabelkategorie
Kabelqualifizierer	Eignung für Netzwerkanwendung untersuchen	normgerechte Zertifizierung
Kabelzertifizierer	Verkabelung gegen definierte Grenzwerte messen	fehlerfreie Switch- oder Endgeräte
TDR	Entfernung zu elektrischer Auffälligkeit bestimmen	genaue mechanische Ursache
Tongenerator	Leitung suchen und zuordnen	Ethernet-Leistungsfähigkeit
Loopback-Stecker	lokalen Sende- und Empfangspfad prüfen	gesamten Ende-zu-Ende-Pfad

Werkzeug	Hauptzweck	bestätigt nicht automatisch
PoE-Tester	PoE-Erkennung und Leistung untersuchen	stabile Leistung ohne Lastmessung
Multimeter	geeignete elektrische Größen messen	sichere Bedienung ohne Qualifikation
Glasfaser-Inspektionssonde	Endflächen untersuchen	optische Dämpfung
Visual Fault Locator	grobe Fehler und Faserzuordnung prüfen	normgerechte Streckenqualität
optischer Leistungsmesser	absoluten Empfangspegel messen	genaue Position einer Fehlerstelle
OLTS	Einfügedämpfung der Strecke messen	genaue Lage einzelner Ereignisse
OTDR	Ereignisse und Entfernungen entlang der Faser analysieren	vollständigen Ersatz für OLTS
Spektrumanalysator	Funkenergie und Störquellen untersuchen	erfolgreiche WLAN-Anmeldung
Wärmebildkamera	Temperaturverteilung sichtbar machen	interne Bauteiltemperatur ohne Einordnung
Konsolenkabel	lokalen Gerätezugriff ermöglichen	funktionierendes Netzwerk
Out-of-Band-Management	unabhängigen Hardware- und Konsolenzugriff bereitstellen	funktionierendes Betriebssystem

Merksatz

“ Physische Fehleranalyse beginnt mit Sichtprüfung, Dokumentation und einem kontrollierten Vergleich. Danach wird das passende Messgerät eingesetzt: Kabeltester für Verdrahtung, Zertifizierer für Übertragungsgrenzen, TDR und OTDR für Fehlerentfernungen, Leistungsmesser für optische Pegel, PoE-Tester für Stromversorgung unter realen Bedingungen und Spektrumanalysator für Funkstörungen. Ein einzelner Messwert ersetzt niemals die technische Einordnung und die abschließende Funktionsprüfung.

Quellen und weiterführende Dokumentation

- [Fluke Networks – Verification, Qualification und Certification unterscheiden](#)
- [Fluke Networks – Kupfer-Kabelzertifizierung mit der DSX CableAnalyzer-Serie](#)
- [Fluke Networks – Versiv Cable Certifier](#)
- [Fluke Networks – Grundlagen der Netzwerk- und Kabelprüfung](#)
- [Fluke Networks – Glasfaser-Messgeräte und Fehlersuche](#)
- [Fluke Networks – Optische Leistungsmesser und Fehlerlokalisierung](#)

- Fluke Networks – OLTS und OTDR als vollständige Prüfstrategie
 - Fluke Networks – OptiFiber Pro OTDR
 - Fluke Networks – Glasfaser inspizieren und reinigen
 - Fluke Networks – Grundregel für Glasfaser: inspizieren, reinigen und erneut inspizieren
 - NetAlly – Funktionsweise von Netzwerk-Kabeltestern
 - NetAlly – Häufige PoE-Probleme erkennen
 - NetAlly – PoE-Prüfung mit einem tragbaren Netzwerkprüfgerät
 - NetAlly – Kabel-, Netzwerk-, WLAN- und Spektrumanalyse
 - Cisco – Out-of-Band-Management: Best Practices
 - Cisco – Integrated Management Controller für UCS-C-Series-Server
-