

1.2 Fehlerumfang mit Kreuztests bestimmen

Zweck dieser Seite

Diese Seite dient dazu, den Umfang einer Störung systematisch einzugrenzen.

Nach der Störungsaufnahme ist bekannt, welches Symptom beobachtet wurde. Jetzt wird geprüft, ob die Ursache wahrscheinlich beim Benutzer, beim Gerät, beim Netzwerk, beim Standort, beim Zielsystem oder bei einem zentralen Dienst liegt.

In dieser Phase wird die Ursache noch nicht behoben. Das Ziel ist zunächst, die Fehlerdomäne möglichst stark zu verkleinern.

Grundprinzip

Ein einzelner Test zeigt häufig nur, dass etwas funktioniert oder nicht funktioniert.

Ein Kreuztest verändert gezielt nur eine Bedingung:

- gleicher Benutzer, anderes Gerät;
- anderer Benutzer, gleiches Gerät;
- gleiches Gerät, andere Netzwerkverbindung;
- gleiches Gerät, anderer Switchport;
- gleiche Quelle, anderes Ziel;
- andere Quelle, gleiches Ziel.

Dadurch lässt sich erkennen, mit welcher Komponente der Fehler mitwandert.

Was ist eine Fehlerdomäne?

Eine Fehlerdomäne ist der technische oder organisatorische Bereich, in dem die Ursache wahrscheinlich liegt.

Mögliche Fehlerdomänen:

Fehlerdomäne	Beispiele
Benutzer	Konto, Passwort, Gruppen, Rollen, Profil oder persönliche Einstellungen
Gerät	Betriebssystem, Treiber, lokale Firewall, Software oder Hardware
Netzwerkinterface	Ethernetadapter, WLAN-Adapter, USB-Adapter oder virtuelle NIC
Verkabelung	Patchkabel, Dose, Patchfeld oder Gebäudeverkabelung

Fehlerdomäne	Beispiele
Switchport	Portkonfiguration, VLAN, Port Security oder Hardwarefehler
VLAN oder Subnetz	DHCP, Gateway, ACL, Routing oder Broadcast-Domain
Standort	Switch, Firewall, WAN, VPN, Provider oder Stromversorgung
Zielsystem	Server, Anwendung, Dienst, Listener oder lokale Firewall
Zentraler Dienst	DNS, DHCP, Active Directory, NTP, Proxy oder Cloud-Dienst
Benutzergruppe	Gruppenrichtlinie, Berechtigung, Lizenz oder Conditional Access
Betriebssystemgruppe	Update, Treiber, Softwareversion oder Sicherheitsrichtlinie
Zeitpunkt oder Last	Backup, Wartungsjob, hohe Auslastung oder geplante Änderung

Die wichtigsten Eingrenzungsachsen

Achse	Fragestellung
Benutzer	Ist nur ein bestimmter Benutzer betroffen?
Gerät	Tritt der Fehler nur an einem Gerät auf?
Interface	Tritt der Fehler nur über Ethernet, WLAN oder VPN auf?
Port	Tritt der Fehler nur an einem Switchport auf?
VLAN	Sind alle Geräte eines VLANs betroffen?
Subnetz	Sind alle Geräte eines IP-Netzes betroffen?
Standort	Ist nur ein Gebäude oder eine Außenstelle betroffen?
Dienst	Ist nur ein bestimmter Dienst betroffen?
Ziel	Ist nur ein bestimmter Server betroffen?
Betriebssystem	Sind nur Windows-, Linux- oder macOS-Systeme betroffen?
Version	Sind nur Systeme mit einem bestimmten Patchstand betroffen?
Zeit	Tritt der Fehler nur zu bestimmten Zeiten auf?
Last	Tritt der Fehler nur bei hoher Nutzung auf?

Betroffen und nicht betroffen dokumentieren

Die nicht betroffenen Systeme sind für die Diagnose genauso wichtig wie die betroffenen Systeme.

Kategorie	Betroffen	Nicht betroffen
-----------	-----------	-----------------

Benutzer		
Geräte		
Betriebssysteme		
Standorte		
Switchports		
VLANs		
Subnetze		
Netzwerkverbindungen		
Anwendungen		
Server		
Zeiträume		

Beispiel:

Kategorie	Betroffen	Nicht betroffen
Benutzer	user	andere Benutzer
Gerät	CLIENT-01	CLIENT-02
Netzwerkverbindung	Ethernet	WLAN
Dienst	interne Dienste	lokale Anwendungen
Standort	Raum 204	Raum 205

Aus diesem Beispiel ergibt sich noch keine endgültige Ursache. Der Fehlerbereich wurde aber bereits auf Ethernet, Verkabelung, Switchport, VLAN-Zuweisung oder die Ethernetkonfiguration des Clients eingegrenzt.

Regel für kontrollierte Kreuztests

Bei einem Kreuztest wird möglichst nur eine Bedingung verändert.

Ungeeignet:

- anderen Benutzer verwenden;
- gleichzeitig das Gerät wechseln;
- zusätzlich WLAN statt Ethernet verwenden;
- gleichzeitig einen anderen Zielservers testen.

Bei diesem Test wurden mehrere Bedingungen verändert. Das Ergebnis ist nicht eindeutig.

Besser:

1. gleicher Benutzer an anderem Gerät;
2. anderer Benutzer am ursprünglichen Gerät;
3. ursprüngliches Gerät über ein anderes Interface;
4. ursprüngliches Gerät an anderem Switchport.

Kreuztest 1 - Gleicher Benutzer an anderem Gerät

Durchführung

Der betroffene Benutzer testet dieselbe Funktion an einem anderen, nachweislich funktionierenden Gerät.

Auswertung

Ergebnis	Wahrscheinlicher Bereich
Fehler tritt auch am anderen Gerät auf	Benutzerkonto, Berechtigung, Rolle, Lizenz, Profil oder zentral gespeicherte Einstellung
Fehler tritt am anderen Gerät nicht auf	ursprüngliches Gerät, lokale Konfiguration, Interface oder Software
Fehler tritt nur an Geräten eines Standortes auf	Standortnetz, Richtlinie oder gemeinsamer Dienst
Ergebnis abhängig vom Betriebssystem	Clientsoftware, Treiber, Richtlinie oder Kompatibilität

Wichtig

Es muss wirklich dieselbe Funktion mit demselben Benutzer getestet werden.

Kreuztest 2 - Anderer Benutzer am gleichen Gerät

Durchführung

Ein anderer berechtigter Benutzer testet dieselbe Funktion am betroffenen Gerät.

Auswertung

Ergebnis	Wahrscheinlicher Bereich
Anderer Benutzer ist ebenfalls betroffen	Gerät, Betriebssystem, Netzwerk oder lokale Software
Anderer Benutzer ist nicht betroffen	Benutzerprofil, Konto, Rechte, Gruppen oder persönliche Einstellungen
Administrator funktioniert, Standardbenutzer nicht	Rechte, UAC, Richtlinie oder Dateiberechtigung
Lokaler Benutzer funktioniert, Domänenbenutzer nicht	AD, DNS, Kerberos, GPO oder Netzwerkerreichbarkeit

Anmeldedaten dürfen nicht zwischen Benutzern weitergegeben werden. Der andere Benutzer meldet sich selbst an.

Kreuztest 3 - Gleiches Gerät über anderes Netzwerkinterface

Mögliche Vergleiche:

- Ethernet gegen WLAN;
- WLAN gegen Ethernet;
- interne Verbindung gegen VPN;
- VPN gegen direkte Standortverbindung;
- integrierte NIC gegen bekannten funktionierenden USB-Netzwerkadapter.

Auswertung

Ergebnis	Wahrscheinlicher Bereich
Ethernet fehlerhaft, WLAN funktioniert	Ethernetadapter, Kabel, Switchport, VLAN oder kabelgebundenes Netz
WLAN fehlerhaft, Ethernet funktioniert	WLAN-Adapter, Funkversorgung, SSID, Authentifizierung oder WLAN-VLAN
Direkter Zugriff funktioniert, VPN nicht	VPN, Tunnelrouting, VPN-DNS, MTU oder Berechtigung
VPN funktioniert, lokaler Standortzugriff nicht	Standortnetz, lokales Routing, Firewall oder DNS
Beide Interfaces fehlerhaft	Betriebssystem, zentrale Dienste, Zielsystem oder allgemeine Konfiguration

Ein funktionierendes alternatives Interface ist ein wichtiger Hinweis, aber noch keine dauerhafte Lösung.

Kreuztest 4 - Gleiches Gerät an anderem Switchport

Durchführung

Das betroffene Gerät wird kontrolliert mit einem nachweislich funktionierenden Port verbunden.

Dabei müssen berücksichtigt werden:

- Port-VLAN;
- Portprofil;
- Voice VLAN;
- Port Security;
- 802.1X;
- NAC;
- DHCP Snooping;
- Geschwindigkeit;

- PoE;
- Trunk- oder Access-Konfiguration.

Auswertung

Ergebnis	Wahrscheinlicher Bereich
Gerät funktioniert am anderen Port	ursprünglicher Port, Portprofil, VLAN, Kabelweg oder Switchhardware
Gerät funktioniert auch am anderen Port nicht	Client, Adapter, Betriebssystem oder übergeordneter Netzwerkdienst
Mehrere Geräte funktionieren am ursprünglichen Port nicht	Port, Kabelweg oder Switchkonfiguration
Andere Geräte funktionieren am ursprünglichen Port	ursprünglicher Client oder dessen Authentifizierung

Der Vergleichsport muss für denselben Einsatzzweck und dasselbe VLAN vorgesehen sein.

Kreuztest 5 - Funktionierendes Gerät am betroffenen Port

Durchführung

Ein bekannt funktionierendes Gerät wird mit dem ursprünglichen Kabel und Switchport verbunden.

Auswertung

Ergebnis	Wahrscheinlicher Bereich
Vergleichsgerät funktioniert	ursprünglicher Client, NIC, Treiber oder Clientkonfiguration
Vergleichsgerät funktioniert nicht	Kabel, Dose, Patchfeld, Switchport, VLAN oder Portprofil
Vergleichsgerät erhält anderes VLAN	802.1X, NAC, MAC-basierte Zuweisung oder Portprofil
Vergleichsgerät erhält ebenfalls keine IP	DHCP, VLAN, Relay, Snooping oder Portkonfiguration

Kreuztest 6 - Gleiches Gerät, anderes Ziel

Durchführung

Vom betroffenen Client werden mehrere technisch vergleichbare Ziele getestet.

Beispiele:

- anderer Server im gleichen VLAN;
- anderer Server im entfernten Netz;
- anderer interner Webdienst;
- öffentliche IP-Adresse;
- interner und externer DNS-Name.

Auswertung

Ergebnis	Wahrscheinlicher Bereich
Nur ein Ziel ist nicht erreichbar	Zielserver, Zieldienst, Ziel-Firewall oder Rückroute
Alle Ziele eines Subnetzes sind nicht erreichbar	Routing, ACL, Firewall oder Gateway dieses Netzes
Interne Ziele funktionieren, externe nicht	WAN, NAT, Proxy, Firewall oder Provider
Externe Ziele funktionieren, interne nicht	internes Routing, VPN, interne DNS-Auflösung oder interne Firewall
Nur ein bestimmter Dienst ist nicht erreichbar	Port, Listener, Host-Firewall oder Anwendung

Kreuztest 7 - Andere Quelle, gleiches Ziel

Durchführung

Dasselbe Ziel wird von einem anderen Client, VLAN oder Standort getestet.

Auswertung

Ergebnis	Wahrscheinlicher Bereich
Andere Quelle erreicht das Ziel	ursprünglicher Client oder ursprünglicher Netzwerkpfad
Keine Quelle erreicht das Ziel	Zielsystem, zentraler Dienst oder allgemeiner Netzwerkpfad
Nur ein VLAN erreicht das Ziel nicht	VLAN-Gateway, ACL, Routing oder Firewallregel
Nur ein Standort erreicht das Ziel nicht	WAN, Standortfirewall, VPN oder Provider
Nur ein Betriebssystem ist betroffen	Clientsoftware, Zertifikat, Richtlinie oder Protokollkompatibilität

Kreuztest 8 - IP-Adresse gegen Hostname

Durchführung

Das Ziel wird zuerst über die IP-Adresse und anschließend über den Hostnamen geprüft.

Prüfung	Windows	Linux	macOS
Ziel-IP testen	[RO] Test-NetConnection <Ziel-IP>	[RO] ping -c 4 <Ziel-IP>	[RO] ping -c 4 <Ziel-IP>
Hostname testen	[RO] Test-NetConnection <Hostname>	[RO] ping -c 4 <Hostname>	[RO] ping -c 4 <Hostname>
DNS-Abfrage	[RO] Resolve-DnsName <Hostname>	[RO] dig <Hostname>	[RO] dig <Hostname>

Auswertung

Ergebnis	Wahrscheinlicher Bereich
IP funktioniert, Hostname nicht	DNS, DNS-Suffix, Clientcache oder hosts-Datei
IP und Hostname funktionieren nicht	Erreichbarkeit, Routing, Firewall oder Zielsystem
Hostname löst auf falsche IP auf	DNS-Record, Split-DNS, Cache oder falscher DNS-Server
A-Record funktioniert, AAAA-Pfad nicht	IPv6-Konfiguration oder IPv6-Routing
Kurzname funktioniert nicht, FQDN funktioniert	DNS-Suffix oder Suchdomäne

Kreuztest 9 - Ping gegen tatsächlichen Dienstport

Ein Ping prüft nicht den eigentlichen Anwendungsdienst.

Prüfung	Windows	Linux	macOS
ICMP	[RO] Test-NetConnection <Ziel>	[RO] ping -c 4 <Ziel>	[RO] ping -c 4 <Ziel>
TCP-Port	[RO] Test-NetConnection <Ziel> -Port <Port>	[RO] nc -vz <Ziel> <Port>	[RO] nc -vz <Ziel> <Port>
HTTPS	[RO] curl -v https://<Ziel>/	[RO] curl -v https://<Ziel>/	[RO] curl -v https://<Ziel>/

Auswertung

Ergebnis	Wahrscheinlicher Bereich
Ping und Port funktionieren	grundlegende Verbindung vorhanden; Anwendung weiter prüfen
Ping funktioniert, Port nicht	Listener, Dienst, Host-Firewall oder Netzwerkfirewall
Ping funktioniert nicht, Port funktioniert	ICMP wird wahrscheinlich gefiltert
Port funktioniert, HTTPS-Anfrage nicht	TLS, Proxy, Host Header oder Anwendung
TCP-Verbindung wird zurückgesetzt	Zielprozess, Firewall, Proxy oder Load Balancer

`curl -v` kann Header, Zertifikatsinformationen und sensible Sitzungsdaten anzeigen. Ausgaben müssen vor der Weitergabe geprüft werden.

Kreuztest 10 - Lokal gegen entfernt

Test	Zweck
Dienst lokal auf dem Server testen	Prüft, ob Anwendung und lokaler Listener funktionieren
Dienst aus gleichem VLAN testen	Prüft den lokalen Netzwerkzugriff
Dienst aus anderem VLAN testen	Prüft Routing und Firewall zwischen Netzen

Test	Zweck
Dienst über VPN testen	Prüft Tunnel, VPN-Routing und VPN-DNS
Dienst aus externem Netz testen	Prüft WAN, NAT, Reverse Proxy oder externe Firewall

Auswertung

Ergebnis	Wahrscheinlicher Bereich
Lokal funktioniert, entfernt nicht	Firewall, Bind-Adresse, Routing, NAT oder Netzwerkpfad
Lokal funktioniert nicht	Dienst, Anwendung, Konfiguration oder Abhängigkeit
Gleiches VLAN funktioniert, anderes VLAN nicht	Inter-VLAN-Routing, ACL oder Firewall
Intern funktioniert, extern nicht	NAT, WAN-Firewall, DNS oder Reverse Proxy
Extern funktioniert, intern nicht	Hairpin NAT, internes DNS oder interne Route

System- und Netzwerkidentität prüfen

Prüfung	Windows	Linux	macOS
Benutzer	[RO] whoami	[RO] whoami	[RO] whoami
Hostname	[RO] hostname	[RO] hostname	[RO] hostname
Interfaces	[RO] Get-NetAdapter	[RO] ip -brief link	[RO] ifconfig -l
IP-Adressen	[RO] Get-NetIPAddress	[RO] ip -brief address	[RO] ifconfig
Standardroute	[RO] Get-NetRoute - DestinationPrefix "0.0.0.0/0"	[RO] ip route show default	[RO] route -n get default
DNS-Server	[RO] Get-DnsClientServerAddress	[RO] resolvectl status	[RO] scutil --dns

Diese Informationen helfen zu prüfen, ob die verglichenen Systeme tatsächlich im erwarteten Netzwerk, VLAN oder Benutzerkontext arbeiten.

Empfohlene Reihenfolge der Kreuztests

1. Betroffenen Benutzer und betroffenes Gerät bestätigen.
2. Anderen Benutzer am gleichen Gerät testen.
3. Gleichen Benutzer an anderem Gerät testen.
4. Gleiches Gerät über anderes Interface testen.
5. Anderes Gerät am gleichen Port testen.
6. Gleiches Gerät an geeignetem Vergleichsport testen.
7. Andere Ziele von gleicher Quelle testen.
8. Gleiches Ziel von anderer Quelle testen.
9. IP-Adresse gegen Hostname testen.
10. Ping gegen tatsächlichen Dienstport testen.

- 11. lokalen, internen und entfernten Zugriff vergleichen.
- 12. Ergebnisse in einer Betroffen/Nicht-betroffen-Matrix festhalten.

Nicht jeder Fehler benötigt alle Kreuztests. Sobald die Fehlerdomäne eindeutig eingegrenzt ist, wird mit der passenden technischen Detailseite fortgefahren.

Auswertungsmatrix

Beobachtung	Wahrscheinliche Fehlerdomäne	Passende Folgeseite
Nur ein Benutzer betroffen	Konto, Rechte oder Profil	Benutzer- und Identitätsdiagnose
Nur ein Gerät betroffen	Client, Treiber oder lokale Konfiguration	Windows-, Linux- oder macOS-Diagnose
Nur Ethernet betroffen	NIC, Kabel, Port oder VLAN	Hardware, Switching und VLAN
Nur WLAN betroffen	Funk, SSID, Authentifizierung oder WLAN-VLAN	WLAN-Diagnose
Nur ein Port betroffen	Switchport, Kabelweg oder Portprofil	Switching und Verkabelung
Nur ein VLAN betroffen	Gateway, DHCP Relay, ACL oder Routing	VLAN, DHCP und Routing
Nur ein Standort betroffen	WAN, VPN, Firewall oder Provider	WAN- und Standortdiagnose
Nur ein Ziel betroffen	Zielserver, Dienst oder Rückroute	Server- und Dienstdiagnose
Nur ein Port oder Protokoll betroffen	Listener oder Firewall	TCP-, UDP- und Firewall-Diagnose
IP funktioniert, Hostname nicht	DNS	DNS-Diagnose
Alle Benutzer und Geräte betroffen	zentraler Dienst oder Infrastruktur	zentrale Infrastruktur prüfen
Fehler tritt nur zu bestimmten Zeiten auf	Last, Job, Wartung oder Timeout	Performance- und Zeitdiagnose

Vorlage zur Dokumentation der Kreuztests

Nummer	Unveränderte Bedingung	Veränderte Bedingung	Ergebnis	Schlussfolgerung
1				
2				
3				
4				
5				

Beispiel

Ausgangssituation

CLIENT-01 erhält über Ethernet keine gültige DHCP-Adresse. Über WLAN funktioniert der Netzwerkzugriff.

Kreuztest	Ergebnis
Anderer Benutzer an CLIENT-01 über Ethernet	ebenfalls betroffen
Ursprünglicher Benutzer an CLIENT-02	funktioniert
CLIENT-01 über WLAN	funktioniert
CLIENT-02 am Port von CLIENT-01	erhält ebenfalls keine DHCP-Adresse
CLIENT-01 an geeignetem Vergleichsport	erhält gültige DHCP-Adresse

Schlussfolgerung

Der Fehler ist nicht benutzerabhängig und wahrscheinlich nicht durch die allgemeine Clientkonfiguration verursacht.

Die Fehlerdomäne wurde auf folgende Komponenten eingegrenzt:

- ursprüngliches Patchkabel;
- Netzwerkdose;
- Patchfeld;
- Switchport;
- Port-VLAN;
- Portprofil;
- DHCP Snooping oder Port Security.

Die weitere Diagnose erfolgt im Kapitel zu Verkabelung, Switching und VLAN.

Nicht vorschnell verändern

Während der Eingrenzung nicht gleichzeitig:

- Benutzerrechte ändern;
- Client neu installieren;
- Netzwerkstack zurücksetzen;
- DNS- oder ARP-Cache löschen;
- Switchport neu konfigurieren;
- VLAN ändern;
- Firewall deaktivieren;
- DHCP-Reservierung löschen;
- Dienste neu starten.

Zuerst muss festgestellt werden, mit welcher Komponente der Fehler zusammenhängt.

Ergebnis dieser Seite

Nach Abschluss der Kreuztests sollte bekannt sein, ob die Störung wahrscheinlich abhängig ist von:

- Benutzer;
- Gerät;
- Netzwerkinterface;
- Kabel oder Switchport;
- VLAN oder Subnetz;
- Standort;
- Betriebssystem oder Version;
- Zielsystem;
- Dienst oder Port;
- DNS;
- VPN;
- Zeitpunkt oder Last.

Die technische Detaildiagnose beginnt anschließend innerhalb der eingegrenzten Fehlerdomäne.

Nächste Seite

1.3 Zeitpunkt und letzte Änderungen untersuchen

Quellen

- [IBM – Systematischer Troubleshooting-Ansatz](#)
 - [Microsoft – Windows Networking Troubleshooting](#)
 - [Microsoft – Test-NetConnection](#)
 - [Cisco – Switchport- und Interfaceprobleme](#)
 - [Apple – Netzwerkprobleme durch Vergleich mit anderem Netzwerk eingrenzen](#)
 - [Red Hat – Netzwerkkonfiguration und Routing](#)
-