Link: https://www.tecchannel.de/a/ratgeber-fehler-im-lan-entdecken,2022717

Tipps und Tricks

Ratgeber - Fehler im LAN entdecken

Datum: 29.06.2013
Autor(en): Jürgen Hill

Netzwerkkabel einstecken und alles funktioniert - leider ist es nicht immer so. Die Fehlersuche kann dann schnell langwierig und nervig sein. Auf welche typischen Fallstricke Sie achten müssen und wie sie diese vermeiden, erläutert dieser Artikel.

In der Theorie funktionieren **Netzwerke**[1] heutzutage problemlos. Irgendwo steht ein DHCP-Server, der automatisch an die angeschlossenen **PCs**[2] eine passende IP vergibt. Wer in einem Unternehmen beispielsweise sein **Notebook**[3] oft in verschiedenen Räumen anstöpselt, schätzt diese automatische Vergabe von IPs.

In vielen Fällen funktioniert der Netzwerkbetrieb, gerade bei einfach aufgebauten Netzen, auch tadellos. Doch mit der Unternehmensgröße wächst auch schnell die Netzwerkkomplexität mit verschiedenen **Switches**[4], Segmenten, diversen **Servern**[5], **Appliances**[6] oder **NAS-Systemen**[7]. Alle Geräte sind im Netzwerk eingebunden und sie bieten oft umfangreiche und komplexe Netzwerkeinstellungen. Ein paar falsche Klicks in den Einstellungen oder ungünstige Default-Werte, und schnell kann das Netzwerk quälend langsam werden oder es funktioniert gleich überhaupt nicht mehr.

Die Fehlersuche im Netzwerk wird schnell komplex, wenn man nicht weiß, wo man anfangen sollte. So paradox es klingt, aber in jedem Netzwerk sollte die Fehlersuche auf der untersten Schicht des OSI-Layers beginnen. Vielleicht hat nur ein Netzwerkkabel einen Ermüdungsbruch erlitten und der Netzwerkkartentreiber funktioniert tadellos.

1. Praxistipp für die Fehlersuche im Netzwerk

Alles ist sorgfältig verlegt und angeschlossen, dennoch streikt das Netz - eine Applikation funktioniert nicht oder die neue Multimedia-Applikation zickt herum. Wer jetzt bei der Fehlersuche falsch vorgeht, verschlimmbessert womöglich das Problem.

Hier hat **D-Link**[8]-Senior Consultant Christoph Becker einen Ratschlag parat, der auf den ersten Blick ungewohnt und fast schon paradox klingt: Egal, ob Heimnetz oder Corporate Network, bei der Fehlersuche sollte der User auf der untersten **Schicht des OSI-Layers**[9], also im Zweifelsfall mit der Netzebene 1 beginnen und sich dann nach oben arbeiten.

[Hinweis auf Bildergalerie: **Fehler im Lan entdecken**] gal1

Üblicherweise würde man im Fehlerfall aber wohl genau andersherum vorgehen, denn auf den oberen komplexeren Netzschichten gibt es ja vielmehr Fehlerquellen. Eine Argumentation, die Becker im Prinzip teilt, gleichzeitig hält er aber entgegen: "Und was haben Sie davon, wenn Sie auf den oberen Ebenen den Fehler suchen, in Wirklichkeit aber ein Kabel einen Ermüdungsbruch hat? Sie haben die doppelte Arbeit, weil sie sich oft mit der Fehlersuche auf der falschen OSI-Ebene auch noch ihre Netzeinstellungen zerschossen haben." Er empfiehlt deshalb, sich bei der Suche unbedingt von der untersten OSI-Ebene nach oben vorzuarbeiten und so Fehlerquellen auszuschließen.

2. Tückische Ethernet-Kabel

Der erste Blick sollte den verwendeten Kabelverbindungen gelten, wie wir aus leidvoller Erfahrung selbst wissen. So brachte uns einmal ein NAS-Test fast zu Verzweifelung: Mit Fast Ethernet erzielten wir Messergebnisse, die im Rahmen des zu erwartenden waren. Schlossen wir dagegen ein Gigabit-Ethernet-Device an, brachen die Leistungen drastisch ein.

Kabeltest: Auch optisch unbeschädigt wirkende Kabel sollten überprüft werden.
Foto: Jetter AG

Eine zeitraubende Überprüfung der Switches und Netzkarten zeigte keine Auffälligkeiten. Erst als wir das optisch unbeschädigte Cat5e-spezifizierte Kabel - das ja mit Fast Ethernet funktionierte - austauschten, war der Spuk vorbei. Da der einfache Kabelaustausch - im Heim- oder Testnetz meist noch problemlos möglich - im Enterprise-LAN nicht so einfach ist, ist die Anschaffung eines Kabeltesters dringend ratsam. Dabei sollte das Testgerät aber auch alle Übertragungsarten (vollduplex, Gigabit Ethernet) beherrschen, die später im Alltag gefahren werden.

3. Ethernet-Treiber

Eine andere tückische Fehlerquelle stellen die Netzwerktreiber für die Interface-Karten dar. Wie die Erfahrung zeigt, verschwinden die seltsamsten Netzfehler mit einem Upgrade der Ethernet-Treiber. Wer auf den Seiten des Motherboard- oder Netzwerkkarten-Herstellers keine neueren Treiber findet, sollte die Flinte nicht gleich ins Korn werfen. Die Chipsatz-Hersteller der Netz-Interfaces offerieren meist aktuelle generische Treiberversionen. Bei Windows-Systemen finden sie den Chipsatzhersteller in der Regel im "Gerätemanager" unter "Netzwerkadapter".

4. Jumbo-Frames

Eine weitere, oft übersehene Performance-Bremse sind die so genannten Jumbo-Frames, also überlange Ethernet-Pakete. In Gigabit-Ethernet-Umgebungen sollen sie - zumindest in der Theorie - die Performance bei der Übertragung großer Dateien oder Multimedia-Files deutlich steigern. In der Praxis passiert allerdings oft das Gegenteil: Deutliche Leistungseinbußen. Die eigentlich clevere Idee der Jumbo-Frames hat nämlich einen Haken: Alle Devices im Netz müssen diese Transferart unterstützen. Erschwerend kommt hinzu, dass dieses Verfahren nicht standardisiert ist, womit in heterogenen Umgebungen Probleme fast programmiert sind. Der Ratschlag lautet deshalb: Deaktivieren Sie die Jumbo-Frames bis Sie die reibungslose Netzkommunikation in allen Betriebszuständen garantieren können. Danach können Sie mit diesem Performance-Booster experimentieren.

5. Netzdesign

Die konsequenteste Fehlervermeidung beginnt für D-Link-Supporter Schmitt allerdings bereits im Vorfeld beim Netzdesign: "Komplexe Netze mit VoIP und anderen Echtzeit-Anforderungen lassen sich nicht einfach mit einem gesunden Halbwissen aufbauen." Hier sei eine konsequente Bedarfsanalyse gefordert, die sich dann im Design niederschlagen müsse. Und dieses sei dann später bei der Umsetzung akribisch zu dokumentieren, denn gerade vergessene Komponenten oder Altlasten würden später häufig für unerklärliche Phänomene sorgen: "Sie ziehen etwa ein Kabel und dürften eigentlich keine Netzanbindung mehr haben, der Rechner bleibt aber weiter munter im Netz." Im genannten Beispiel entpuppte sich ein längst vergessener Hub als Übeltäter.

6. Loop im Netz

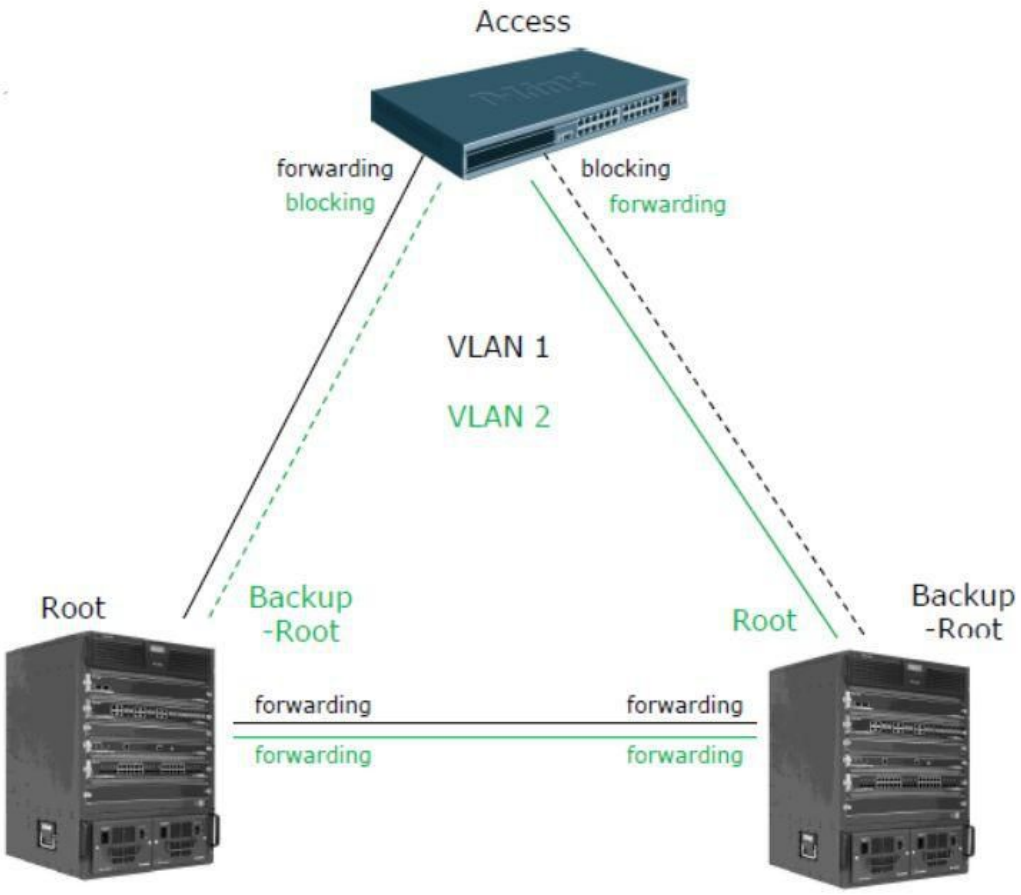
Ein anderer typischer Fallstrick lauert für Schmitt in den so genannten gewachsenen Netzen - also LANs oder Corporate Networks, die je nach Bedarf von Zeit zu Zeit erweitert werden. Oft werden hier nachträglich Kabel gezogen, die dann später zu den krudesten Phänomen führen, wenn die Installation nicht sauber dokumentiert wurde. So können etwa Schleifen (Loops) im Netz entstehen, die dann ein Switched Network, das eigentlich auf dedizierten Verbindungen basiert, ausbremsen. Denn ein solcher Loop verursacht einen Broadcast-Sturm, der ein ganzes Netzsegment lahmlegen kann. Um das Problem zu vermeiden, hat der Netzbetreuer zwei Optionen: Das Aktivieren des Spanning Tree Protcols (STP), das aber oft von Unmanaged Switches nicht unterstützt wird, oder die Verwendung einer Loopback Detection (LBD), wie sie von verschiedenen Herstellern unter diversen Bezeichnungen offeriert wird. Hotline-Supporter Schmitt bevorzugt das LBD-Verfahren, denn der Spanning Tree wartet noch mit einigen Tücken auf - doch dazu später mehr. Bei der Loopback Detection ist dann zwischen einem Port- und VLAN-basierenden Verfahren zu unterscheiden. Während ersteres den Port komplett abschaltet, blockiert letzteres den Verkehr nur im **VLAN**[10], ohne den ganzen Port zu sperren.

7. Fehlende Segmentierung

Gerade diese Segmentierung ist ein Grund, warum der Einsatz von**VLANs**[11] empfohlen wird: Sie erhöhen nicht nur die Sicherheit, sondern begrenzen Störungen auf ein Netzsegment. So blieben beispielsweise Broadcast-Stürme auf ein virtuelles LAN-Segment begrenzt und zögen nicht die gesamte Infrastruktur in Mitleidenschaft.

Allerdings bergen die VLANs in Kombination mit dem Spanning Tree Protocol (STP) auch eine Gefahr. Es kommt durchaus vor, dass das STP ein VLAN deaktiviert, wenn es um Redundanzen zu vermeiden eine physikalische Netzverbindung abschaltet. Auf den ersten Blick erscheint dieses Phänomen unverständlich, doch die Erklärung wird deutlich, wenn man das theoretische Konzept hinter STP betrachtet. Ursprünglich wurde STP entwickelt, um in geswitchten Umgebungen zwei sich widersprechende Anforderungen zu realisieren: Zum einen die Vermeidung mehrfacher Netzpfade zum Ziel, um eine Verdoppelung der Datenpakete zu verhindern; zum anderen die gleichzeitige Redundanz der Netzpfade; um beim Ausfall einer Strecke eine alternative Verbindung zu haben.

Spanning Tree: Erhöht zwar die



Ausfallsicherheit, ist aber eine zusätzliche Fehlerquelle. (Quelle: D-Link)

Genau diese Steuerung übernimmt STP beziehungsweise das Rapid Spanning Tree Protocol (RSTP) als neuere Variante. Hierzu kommunizieren die Switches über das Bridge-Protokoll miteinander. Zuerst wird eine sogenannte Root Bridge bestimmt, die das Oberkommando übernimmt und Startpunkt des Verbindungsbaumes (Tree) ist. Root wird normalerweise die Bridge mit der niedrigsten ID, die sich aus Priorität und MAC-Adresse ergibt. Existieren redundante Wege, so nehmen die **Switches**[12] den Port mit den geringsten Pfadkosten zur Root Bridge und deaktivieren die anderen Ports, darunter eventuell auch ein VLAN.

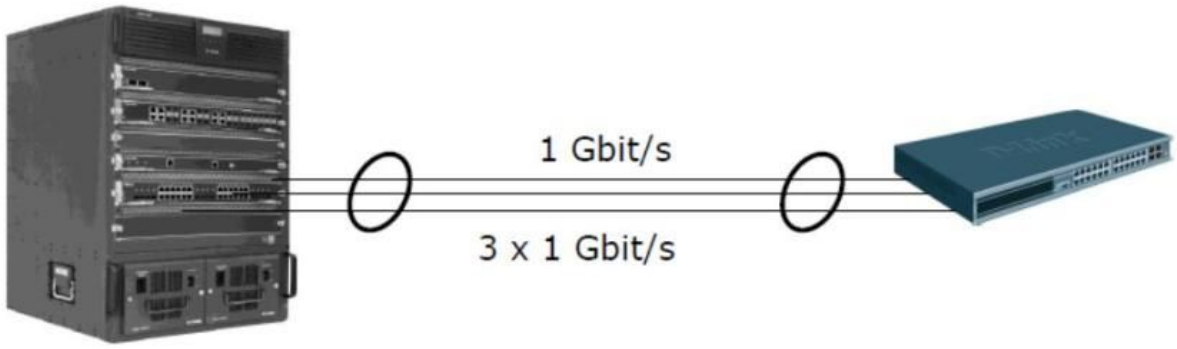
Zudem weist das Konzept, sieht man einmal von Umschaltzeiten von bis zu 30 Sekunden ab (RSTP etwa eine Sekunde), im Fall einer Störung noch zwei andere gravierende Nachteile auf: kommt etwa ein neuer Switch in das Netz, dann kann dieser eventuell aufgrund seiner ID die Aufgabe der Root Bridge automatisch übernehmen und die ursprünglichen Verbindungszuordnungen stimmen nicht mehr, was zu Performance-Problemen führen kann. Ebenso kann es passieren, dass bei einem Ausfall ein Switch die Root-Bridge-Funktion übernimmt, der so ungünstig positioniert ist, dass das Netz zusammenbricht. Eine weitere Gefahr stellen in gewachsenen Netzen neue, ergänzende Kabel dar, die womöglich die Struktur des Spanning Trees zerstören, da sich keine eindeutigen Pfadkosten berechnen lassen.

Angesichts dieser Fallstricke wird geraten, den Spanning Tree nicht sich selbst zu überlassen, sondern etwa für einen Ausfall eine Ersatz-Root-Bridge selbst festzulegen. Wer mit VLANs arbeitet, sollte zudem überlegen, ob er nicht mit dem Multiple Spanning Tree Protocol (MSTP) arbeitet. Dieses wird den Anforderungen der VLANs besser gerecht, da es in einem LAN mehrere Instanzen des Spanning Tree erlaubt. Für Anwender, die mit Hilfe des Spanning Tree einen Ring zur Erhöhung der Ausfallsicherheit nachbilden wollen, hat Schmitt noch einen anderen Ratschlag: Statt auf STP oder RSTP zu setzen, empfiehlt er herstellerspezifische Verfahren - bei D-Link etwa das Rapid Ethernet Ring Protection (RERP) - zu verwenden, da diese teilweise mit Umschaltzeiten von 200 Millisekunden aufwarten und die spezifischen STP-Nachteile nicht haben.

8. Ungenutztes Trunking-Potenzial

Kommt es zu Engpässen im Backbone oder bei Serveranbindungen, stellt sich häufig die Frage nach einem Upgrade auf 10 Gigabit Ethernet. Doch dies ist teuer, so dass viele Unternehmen die Investition scheuen und die entsprechenden Verbindungen am Anschlag fahren. Dabei gibt es eine Alternative: Mit Hilfe des Trunking, also dem parallelen Benutzen von 1 Gigabit/s-Verbindungen, kann die Bandbreite auf diesen Strecken erhöht werden. Üblich sind heute Trunks mit bis zu acht parallelen Verbindungen, was einer Bandbreite von 8 Gigabit/s entspricht.

Mehr



Speed: Es muss nicht immer gleich zehn Gigabit Ethernet sein, die Bandbreite lässt sich auch per Trunking erhöhen. (Quelle: D-Link)

Beim Trunking wird allerdings gerne Potenzial verschenkt: Das Trunking kann nicht nur zur Performance-Steigerung, sondern auch zur Erhöhung der Redundanz genutzt werden. Das Stichwort lautet hier Cross Trunking. Hierbei werden die Ethernet-Kabel etwa zwischen zwei Stacks (Zusammenschluss mehrerer **Switches**[13] zu einem logischen Switch) nicht parallel sondern über Kreuz zwischen den einzelnen Geräten geschaltet, um so bei einem Ausfall möglichst geringe Beeinträchtigungen zu haben.

9. Performance-Falle Priorisierung

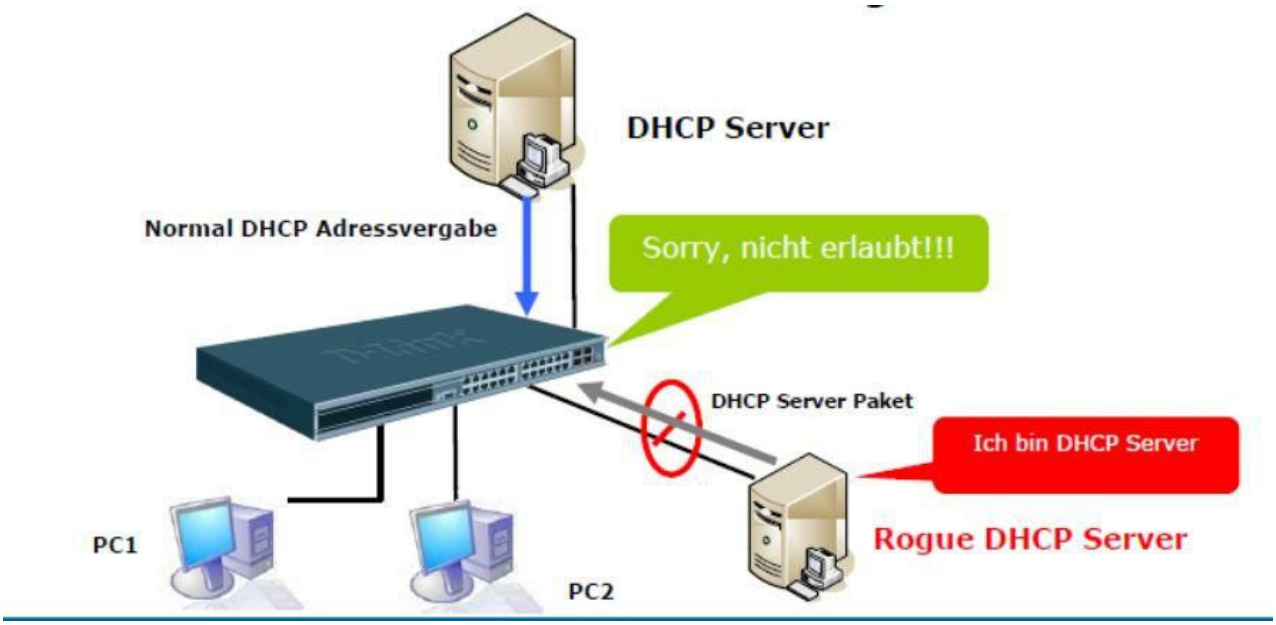
Es ist ein Irrglaube, dass in den heutigen Netzen mit genügend Bandbreite jedes Problem gelöst werden kann. Gerade bei Echtzeitanwendungen wie VoIP oder Video seien zudem Parameter wie Delay, Jitter oder Paket Loss von Bedeutung. Bandbreite ist kein Ersatz für Priorisierung. Bei der Priorisierung ist allerdings darauf zu achten, dass diese im gesamten Netz Ende zu Ende genutzt wird. Wird etwa nur vom VoIP-Telefon in der lokalen Arbeitsgruppe bis hin zum ersten Switch eine Priorisierung gefahren, dann sollte sich niemand wundern, wenn es später dennoch zu Ausfällen kommt. Ebenso wichtig ist, dass alle beteiligten Geräte die Priorisierungsmechanismen auch wirklich unterstützen.

10. Device-Missbrauch

In diesem Zusammenhang gibt es noch eine andere Systembremse, die häufig unterschätzt wird: Der Missbrauch von Endgeräten für Einsatzzwecke, für die sie eigentlich nicht konzipiert wurden. Gerade die langen Feature-Listen aktueller Hardware verleiten oft dazu, zu viele beziehungsweise falsche Aufgaben auf einem Gerät erledigen zu wollen. Ein klassisches Beispiel hierfür ist ein WLAN-Access-Point. Die eigentliche Aufgabe des Geräts sei ein reibungsloser Transport der Daten per Funk. "Deshalb sollte ein Access Point als Access Point", so der D-Link-Supporter Schmitt, "und ein Edge Device wirklich als Edge Device genutzt werden." Wer die Geräte mit ungeeigneten Aufgaben belaste, müsse sich nicht wundern, wenn hinterher die Performance leide. So gehört für Schmitt etwa das Routing in den Core- und nicht in den Edge-Bereich.

11. TCP/IP-Bremse

Etliche unerklärliche Netzphänomene haben ihre Ursache allerdings auch auf den oberen Netzebenen: Doppelt vergebene IP-Adressen können zu den wildesten Fehlern führen. Eine Ursache hierfür sind häufig nicht erlaubte DHCP-Server im Netz, die eigenmächtig Adressen vergeben. Ob diese Server nun aus Versehen entstehen, weil ein neues Gerät per se mit aktiviertem DHCP-Server ausgeliefert wird, oder bewusst von einem User installiert werden, sei dahingestellt.



Störenfriede: Unerlaubt installierte DHCP-Server stören den Netzbetrieb. (Quelle: D-Link)

Als Abhilfe hilft hier ein DHCP Server Screening, das DHCP-Pakete erkennt und im Bedarfsfall automatisch den entsprechenden Netz-Port abschaltet. Ebenfalls oft zu beobachten ist, dass Anwender ihren Rechnern selbst IP-Adressen geben, ohne zu wissen, dass sie damit komplette Netzsegmente lahm legen können. Um dies zu verhindern, empfehlen sich Switches, die das Anlegen von White Lists erlauben, in denen eine IP-Adresse fest einer MAC-Adresse und einem Switch-Port zugeordnet ist. Kommt nun ein Datenpaket mit der falschen Zuordnung - bei D-Link nennt man diese Technik beispielsweise IP-MAC-Port-Binding (IMPB), dann blockiert der Switch den Weitertransport.

12. Fazit - Vorbeugen statt heilen

Unabhängig von diesen Detaillösungen hat D-Link-Supporter Marcus Schmitt für alle Anwender noch einen grundsätzlich Ratschlag auf Lager: "Dokumentieren Sie den Aufbau ihres Netzes penibel genau". Denn diese Dokumentation ist später bereits die halbe Miete bei der Fehlersuche oder hilft bei Erweiterungen, Störungen zu vermeiden, da eventuelle Wechselwirkungen teilweise bereits beim Blick in die Dokumentation ersichtlich sind.

Last, but not least, sollte sich jeder Anwender fragen, was ihn ein Netzausfall wirklich kostet. So wird ein Unternehmen in die Ausfallsicherheit eines LANs im Börsensaal - dessen Ausfall den Ruin bedeuten kann - sicherlich mehr investieren als in das LAN der Verwaltung, wo die Auswirkungen nicht so gravierend sind. (cvi)

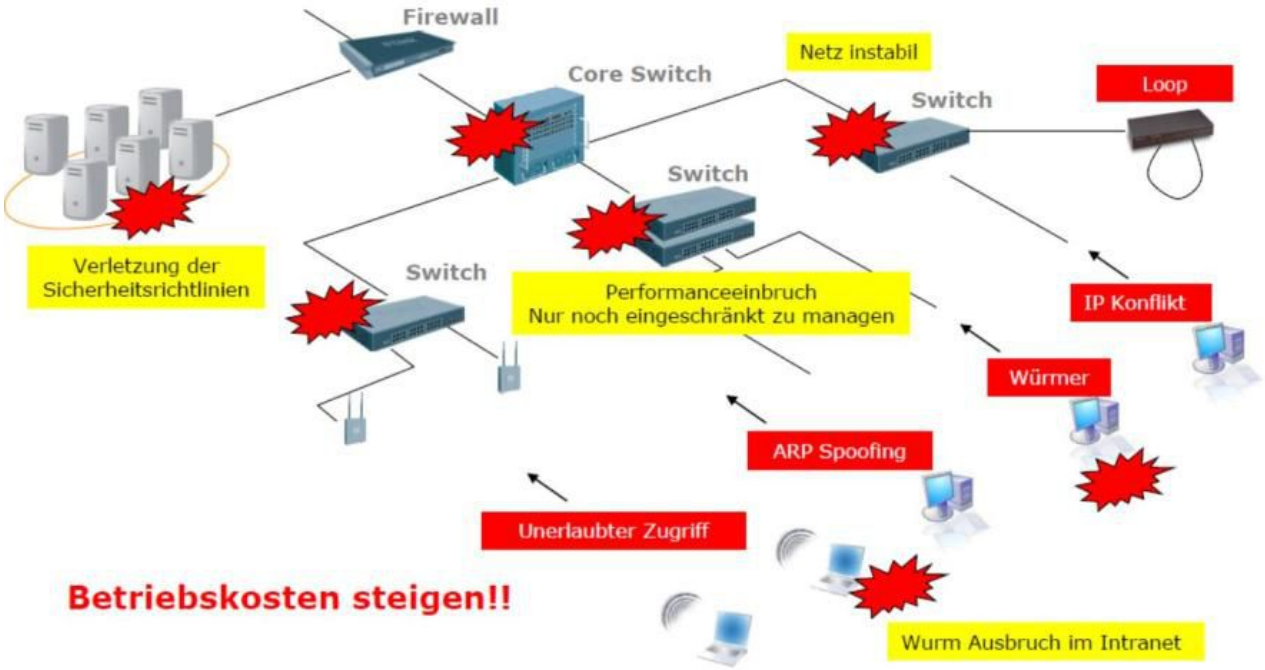
Dieser Artikel basiert auf einem Beitrag von **Computerwoche**[14].

Links im Artikel:

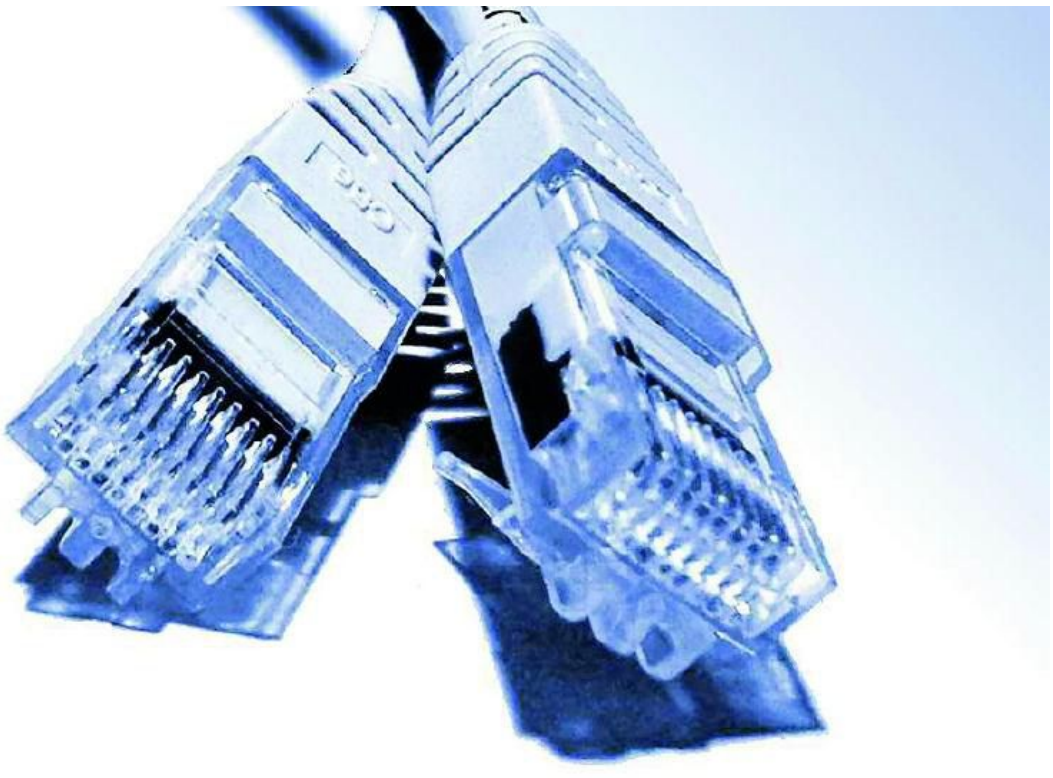
[1] **https://www.tecchannel.de/netzwerk/**
[2] **https://www.tecchannel.de/produkte/pc-mobil/business-pc/**
[3] **https://www.tecchannel.de/produkte/pc-mobil/notebooks/**
[4] **https://www.tecchannel.de/produkte/netzwerk/switches/**
[5] **https://www.tecchannel.de/produkte/server/rack-server/**
[6] **https://www.tecchannel.de/produkte/sicherheit/e-mail-security-appliances/**
[7] **https://www.tecchannel.de/produkte/storage/network-attached-storage-nas/**
[8] **http://www.dlink.de/cs/Satellite?c=Page&childpagename=DLinkEurope-DE/DLGlobalLandingDetail&cid=1197318956476&p=1197318956476&pagename=DLinkEurope-DE/DLWrapper**
[9] **https://www.tecchannel.de/netzwerk/management/402474/netzwerk_basiswissen_teil_3/index3.html**
[10] **https://www.tecchannel.de/netzwerk/lan/434093/einfuehrung_in_vlans_teil_1/**
[11] **https://www.tecchannel.de/netzwerk/lan/434093/einfuehrung_in_vlans_teil_1/**
[12] **https://www.tecchannel.de/produkte/netzwerk/switches/**
[13] **https://www.tecchannel.de/produkte/netzwerk/switches/**
[14] **https://www.computerwoche.de/netzwerke/tk-netze/1902914/**

Bildergalerien im Artikel:

gal1 **Fehler im Lan entdecken**

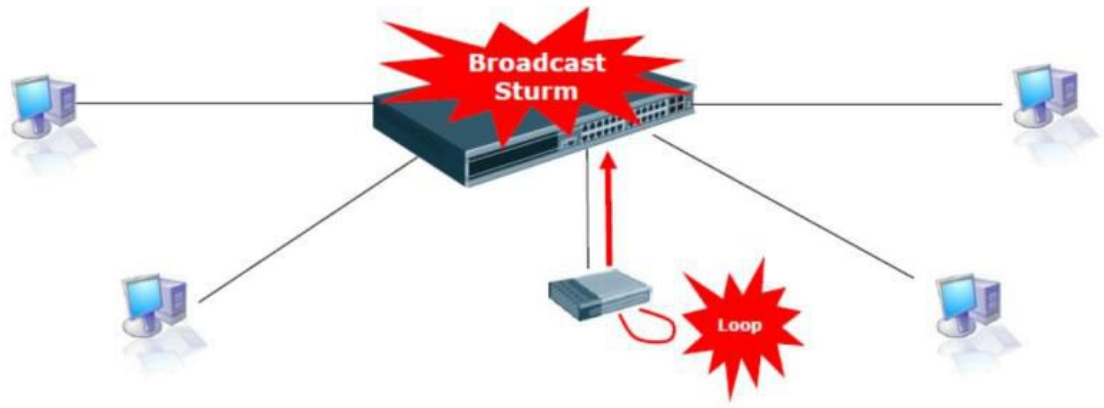


Problemfelder im LAN
Wenn das LAN verrückt spielt, kann das mehrere Gründe haben.



Verbindungsfragen
Als erstes sollten bei LAN-Problemen die Kabel überprüft werden, selbst optisch einwandfreie Kabel können defekt sein.
Foto: sxc.hu, eNex

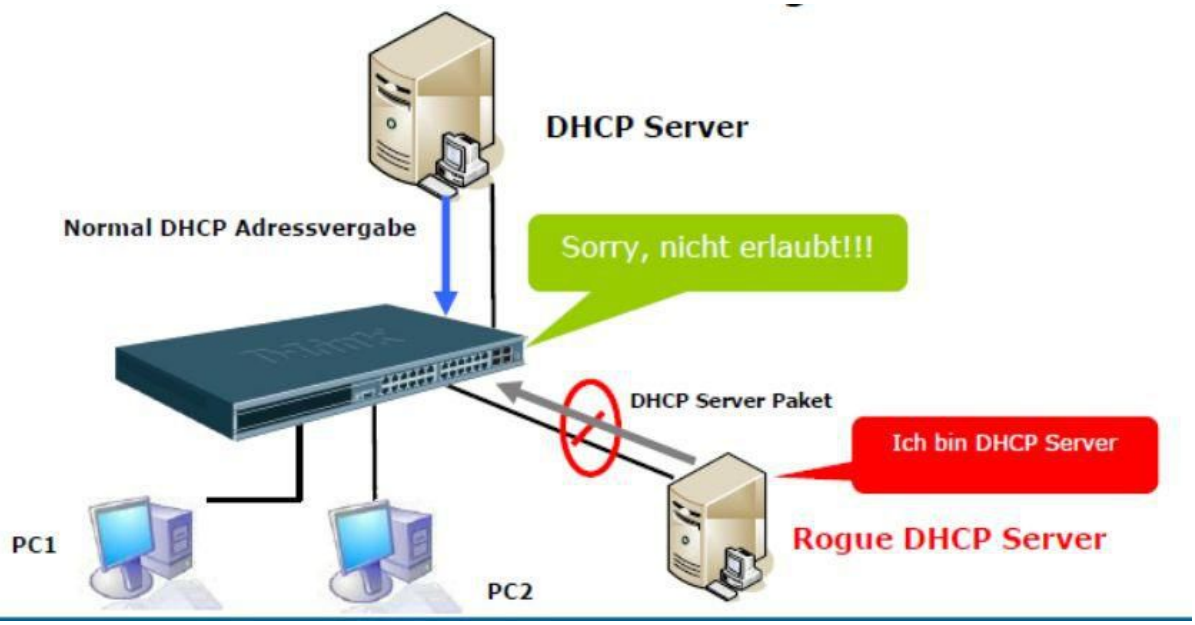
In der



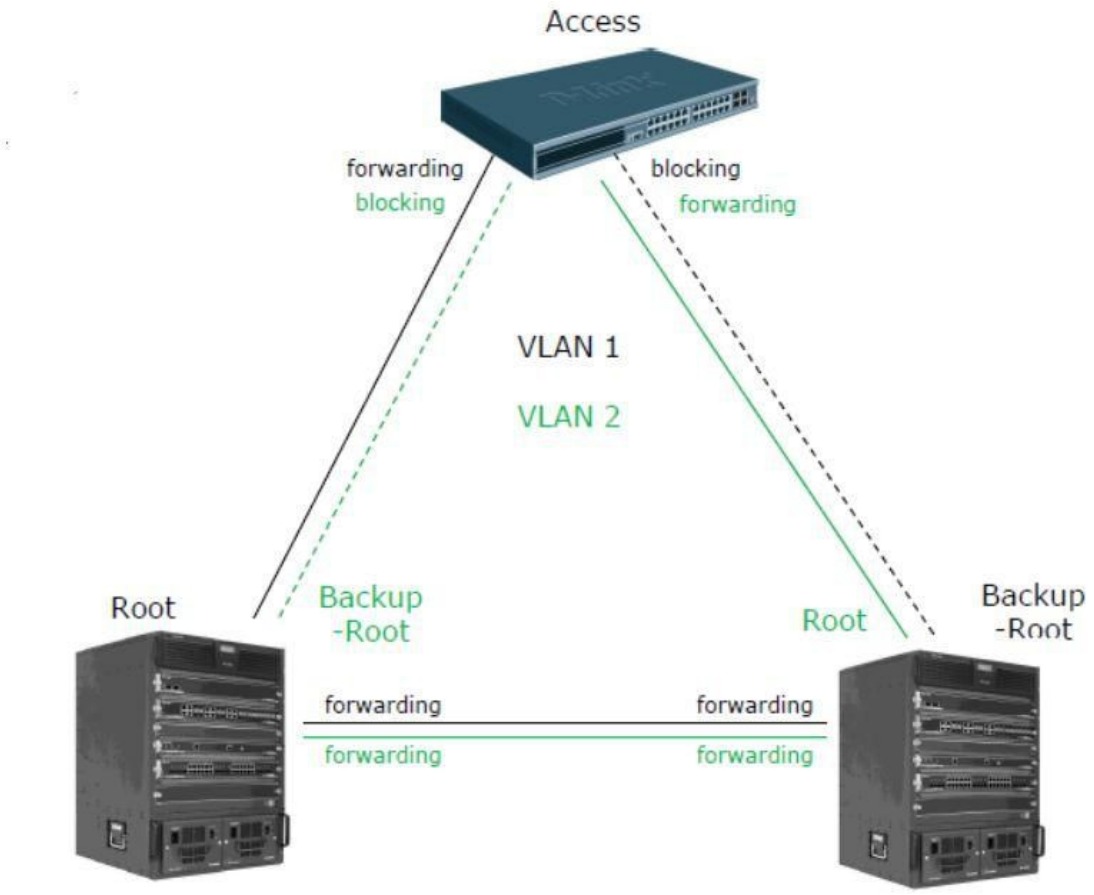
Dauerschleife
Falsch installierte Switches könne für eine Loop sorgen, der Broadcast-Stürme hervorruft. Dieser zusätzliche Verkehr kann das Netz massiv beeinflußen.

Unerlaubte IP-Adressen
Ein weitere beliebte Fehlerquellen sind doppelte oder falsche IP-Adressen. Bei modernen Switchen lassen sich diese Übeltäter auf Port-Ebene aussperren.

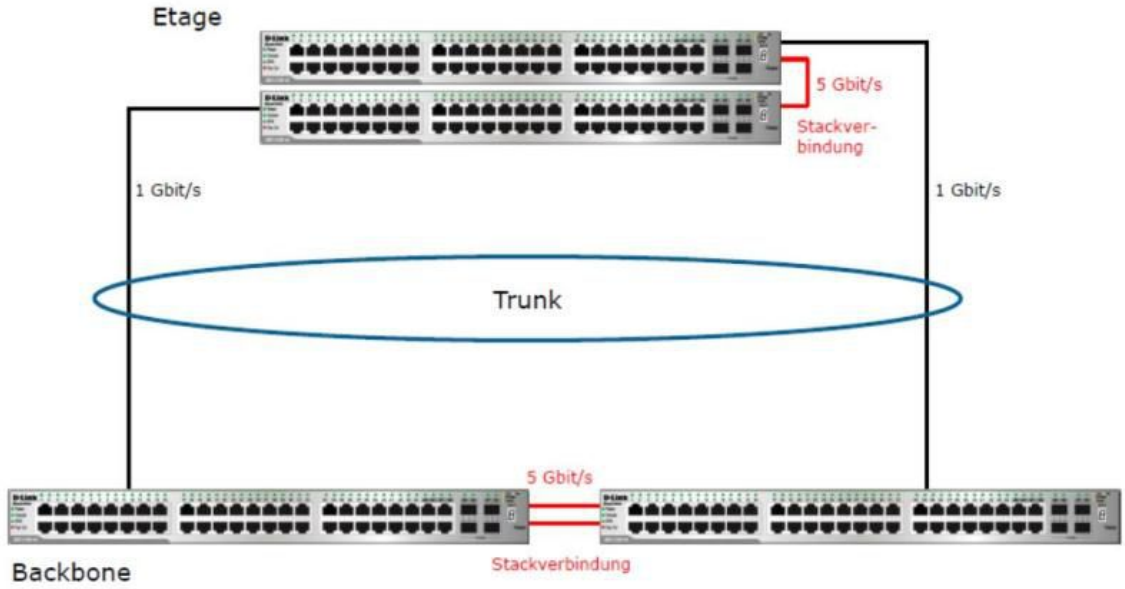
Zu viele



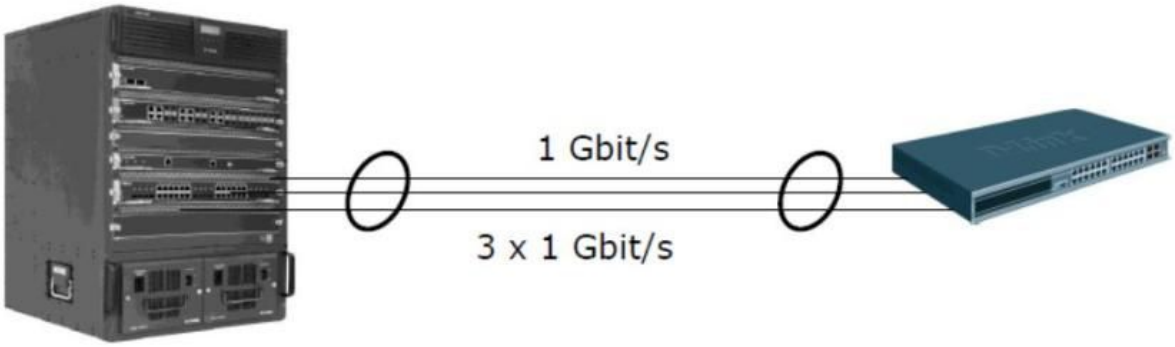
DHCP-Server
Heimlich installierte DHCP-Server finden Sie mit einem Server-Screening. Da das mehrfache Vorhandensein von DHCP-Servern den Netzbetrieb beeinträchtigt, sollten Sie die Störenfriede aussperren.



Fehlerfalle Spanniung Tree
Das Vermeiden von doppelten Strecke und Gewährleistung der Redundanz – diese Vorteile sprechen für ein Netz mit Spanning Tree. Wer jedoch nicht aufpasst handelt sich mehr Probleme ein.



Performance-Booster Trunk
Mit paralellen Leitungen (Trunk) läßt sich die Übertragungsleistung verdoppeln.



Tuning statt Upgrade

Mit Hilfe des Trunking lässt sich häufig ein kostspieliges Upgrade auf 10 Gbit/s Ethernet vermeiden, denn im Trunk können bis zu acht Gigabit-Verbindungen zusammengeschaltet werden.
