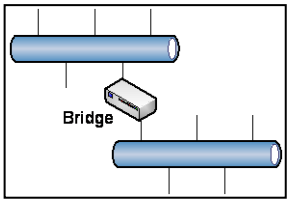
Whitepaper: Loopback Detection (LBD)

Eine strukturierte Verkabelung ist in Firmen heutzutage fast immer vorzufinden. Ebenso oft ist allerdings die Anzahl verfügbarer Anschlüsse bereits erreicht und eine Nachverkabelung wird extrem teuer, da Wanddurchbrüche gemacht werden müssen oder bei existierenden Durchführungen der Brandschutz geöffnet werden muss. Um aus dieser Misere so günstig wie möglich heraus zu kommen, werden in den Büros kleine (Mini-)Switche installiert. Darüber können 5 oder mehr Ports zusätzlich zur Verfügung gestellt werden. Zusätzlich besteht aber auch die Gefahr, dass durch derlei Lösungen Fehlerquellen im Netz entstehen. Durch falsches Patchen (Verbindungen an den Miniswitchen) können Netzwerke zum kompletten Stillstand gebracht werden. Die kleinen Switche sind meist nicht administrierbar, somit können Fehler nicht gesehen werden.

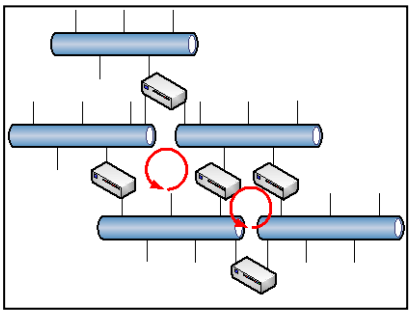
Im Normalfall kann ein Fehlpatchen, durch welches Ringe oder Loops entstehen, vom Netzwerk durch das Spanning Tree Protokoll verhindert werden. Passiert ein solcher Fehler allerdings hinter einem nicht administrierbaren Mini-Switch, so kann dies nicht verhindert werden. Dies erfordert eine weitere Funktionalität: **D-Link Loopback Detection**.

Spanning Tree – „Der Baum im Netzwerk" oder „Ein Ausflug in die Vergangenheit"

Im Ethernet sind prinzipiell keine redundanten Verbindungen erlaubt – ein Ring, nichts anderes stellt eine redundante Verbindung im Ethernet zunächst einmal dar, erzeugt einen sogenannten Loop. Datenpakete fangen dabei an zu kreisen und die Netzwerkperformance bricht augenblicklich zusammen. Aus diesem Grund wurde das Spanning Tree Protokoll entwickelt. Mit Hilfe dieses Protokolls werden automatisch Netzstrukturen gebildet, in welchen redundante Verbindungen so lange geblockt werden, bis eine der aktiven Verbindungen ausfällt. Passiert dies, wird die geblockte Verbindung aktiv geschaltet und der Datenverkehr kann darüber fließen. Auch können Fehlkonfigurationen und daraus resultierende Loops verhindert werden.

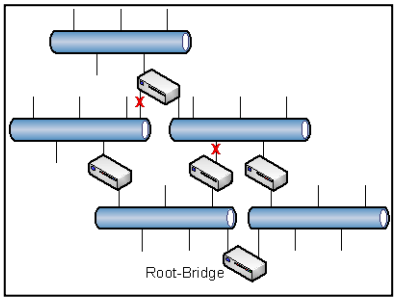


Die Ursprünge des Spanning Tree Protokolls (STP) stammen noch aus der Zeit der Bridges. Diese haben unterschiedliche Ethernetsegmente miteinander verbunden. Die Daten, die auf einem Port dieser Bridges eintreffen, werden auf allen benachbarten Ports wieder ausgegeben. Demzufolge entstand ein Loop, sobald zwischen zwei Ethernetsegmenten eine weitere Verbindung über eine Bridge hergestellt wurde. Aus Redundanzgründen war aber genau dies erwünscht, um bei Ausfall der einen Verbindung die Zweite als Ersatzweg nutzen zu können. Mit Hilfe des Spanning Tree Protokolls wurde dies ermöglicht.



In dem rechts zu sehenden Netz wurden mehrere redundante Wege eingerichtet. Die (ohne Spanning Tree) daraus entstehenden Loops sind als rote Kreise erkennbar. Datenverkehr, der auf der einen Seite „hoch" geschickt wird, kommt auf der anderen Seite wieder herunter, wird wiederum nach oben geschickt usw. Das alles passiert mit der vollen zur Verfügung stehenden Geschwindigkeit.

Nach den Bridges (auch Hub oder Konzentrator genannt) kamen die Switches. Diese brachten den Vorteil, dass der Datenverkehr nicht mehr komplett in alle Segmente verteilt wurde. Jeder Switch baut eine eigene Tabelle auf (Forwarding Database oder FDB), in welcher jeder Teilnehmer im Netz mit seiner MAC-Adresse hinterlegt ist und hinter welchem Port diese zu finden ist. Somit wurde der Datenverkehr sehr stark minimiert, weil die Daten nur noch dahin geschickt wurden, wo sie auch wirklich benötigt werden. Natürlich musste Broadcast Verkehr, wie z.B. ARP-Anfragen, weiter auf alle Ports dupliziert werden. Somit können auch in geswitchten Netzen Loops entstehen. Ein Broadcast reicht hierbei aus, um das Netzwerk zum Erliegen zu bringen.



Wird nun das Spanning Tree Protokoll in einem Netzwerk eingeschaltet so generiert sich eine Netzstruktur, die wegen ihrer Ähnlichkeit zur „Verästelung" auch Baum genannt wird. Sie hat eine sogenannte Root-Bridge als zentralen Punkt (Root = Wurzel). Die Root-Bridge wird anhand der, bei managebaren Switches einstellbaren, Bridge-Priority automatisch ausgewählt. Die Bridge mit der niedrigsten Priority wird „Root". Auf diese Root-Bridge aufbauend bildet sich eine Struktur ohne

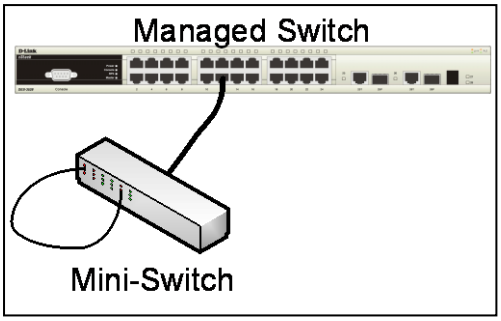
Whitepaper: Loopback Detection (LBD)

Loops. Redundante Verbindungen werden hierbei in einen geblockten Zustand versetzt und leiten keinen Datenverkehr weiter. Fällt nun eine der aktiven Verbindungen aus, wird automatisch eine der geblockten Verbindungen auf „forwarding" gesetzt und somit der redundante Weg frei geschaltet.

Spanning Tree in seiner Implementierung nach 802.1d benötigt etwa 50 Sekunden bis eine Minute um zu konvergieren, das bedeutet, einen definierten, stabilen Zustand des Netzes herzustellen. Bei einem Ausfall einer der Verbindungen bedingt das eine „Downtime" des Netzes von etwa einer Minute. In heutigen Umgebungen ist diese lange Ausfallzeit nicht mehr vertretbar. Aus diesem Grund wurde 802.1d vom „Rapid Spanning Tree", 802.1w, abgelöst. Dieser benötigt in den meisten Fällen nur noch wenige Sekunden, um die redundanten Strecken im Bedarfsfall aktiv zu schalten.

Loops trotz Spanning Tree

Das Spanning Tree Protokoll hat auch seine Grenzen. Werden Loops hinter Netzkomponenten erzeugt, welche kein Spanning Tree unterstützen, so wird dies vom Netzwerk nicht registriert und somit nicht verhindert. Kreisende Datenpakete strahlen wieder auf das ganze Netzwerk aus und bringen dieses zum Ausfall. Dies ist bedingt in der Verarbeitung der sogenannten BPDU Pakete (Bridge Protocol Data Units), welche zur Steuerung des Spanning Tree Protokolls eingesetzt werden.



Häufig werden kleine 5- oder 8-Port Switche verwendet, um z.B. in Büros fehlende Netzwerkanschlüsse bereit zu stellen. Eine Neuinstallation und Neuverkabelung von Netzwerkdosen in Bodentanks oder Wandleisten ist sehr teuer – da dienen Mini-Switche als kostengünstige Alternative. Sind diese Switche nicht konfigurierbar (= unmanaged), so hat ein Netzwerkadministrator keine Möglichkeit, angeschlossene Geräte zu überwachen und Fehler zu entdecken. Gerne werden in solchen Installation beispielsweise Patchkabel, welche nicht angeschlossen auf dem Boden liegen, unter der Annahme, dass noch ein Anschluss fehlt, in einen verfügbaren Port des Mini-Switches gesteckt. War dieses Kabel aber bereits an dem erwähnten Switch angeschlossen, hat man einen klassischen Loop gesteckt. Ohne automatische Hilfsmaßnahmen wird ein Netzwerk, auch wenn es Spanning Tree nutzt, zum Erliegen gebracht.

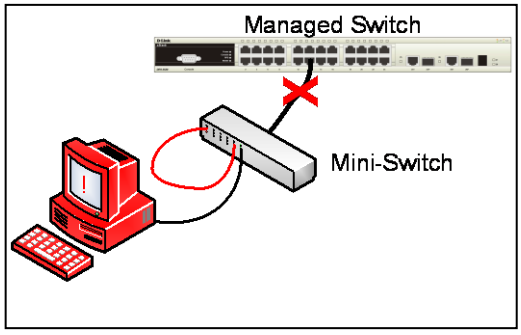
Stabilität durch aktive Überwachung

Um auch in solchen Fällen ein Netzwerk stabil und ausfallsicher zu halten hat D-Link das Feature Loopback Detection (LBD) in seinen xStack Switches implementiert. Mit Hilfe dieser Funktion überwachen die Switches aktiv die an ihnen angeschlossene Netzwerk Infrastruktur auf mögliche Loops. Hierzu verwenden sie Multicast Pakete, welche sie zyklisch auf den aktiven Ports, auf welchen LBD konfiguriert ist, senden. Empfängt ein Switch sein eigenes Multicast Paket auf dem Port, auf dem er es gesendet hat, muss er annehmen, dass sich hinter diesem Port ein Loop befindet.

Hat der Switch auf diese Weise einen Loop festgestellt, so kann er auf zwei unterschiedliche Arten reagieren:

Erste Möglichkeit:

Der betroffene **Port wird komplett abgeschaltet**. Hierbei ist keine Datenkommunikation über diesen Port mehr möglich und der Loop hat keine Auswirkung mehr auf das gesamte Netzwerk. Das gibt dem Netzwerkadministrator Zeit, die Fehlerursache zu finden. Der Switch kann hierzu eine Meldung an ein Netzwerkmanagement System wie zum Beispiel D-View senden.

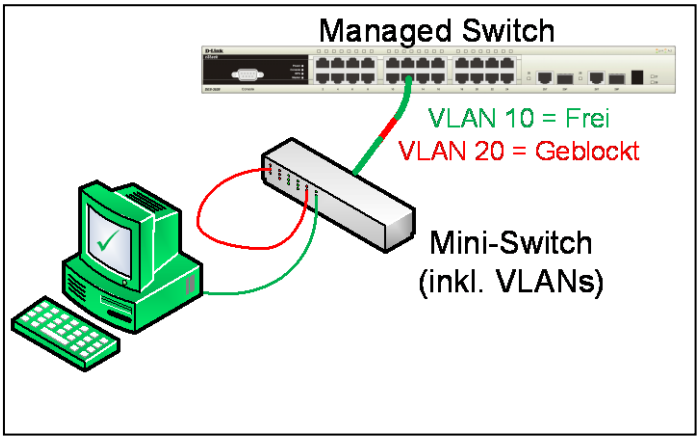


Wie auf dem Bild zu erkennen werden Rechner, die sich über den Loop verursachenden Mini-Switch angeschlossen sind, von dem Rest des Netzes isoliert, sobald Loopback Detection den Port blockt.

Whitepaper: Loopback Detection (LBD)

Zweite Möglichkeit:

Durch die Verwendung unterschiedlicher VLANs kann der Netzwerkverkehr in mehrere Segmente aufgeteilt werden. Kommt es auf einer Komponente in einem VLAN zu einem Loop, so bietet Loopback Detection die Funktionalität, **nur den Datenverkehr für dieses VLAN abzuschalten**. Das hat den entscheidenden Vorteil, dass der Verkehr in den restlichen VLANs unterbrechungsfrei weiterlaufen kann.



Durch den Einsatz von z.B. Smart Switches, welche bereits VLAN Unterstützung beinhaltet haben, kann somit die Auswirkung eines Loops noch einmal minimiert werden.

Stabilität und Verfügbarkeit im Netzwerk

Moderne Netze müssen performant, stabil und verfügbar sein. Gleichzeitig muss aber die Flexibilität und Ausbaufähigkeit gewährleistet sein. Loopback Detection bildet hierbei ein wichtiges Element, um Netzwerken diese Eigenschaften einzuräumen und gibt dem Administrator ein nützliches Werkzeug an die Hand, um Fehler schnell erkennen und lokalisieren zu können, sowie um Netzwerke nach einer Störung schnell wieder zum Einsatz zu bringen.

Loopback-Detection kann hierbei in unterschiedlichen Szenarien mit und ohne VLANs zum Einsatz kommen und bietet dabei größtmögliche Flexibilität. Es ist einfach einzurichten und ist in vielen unterschiedlichen Switches von D-Link verfügbar.

Sicherheitskonzept mit D-Link

Loopback-Detection bildet zusammen mit weiteren, von D-Link in den xStack Switches implementierten Funktionen, wie zum Beispiel IP-MAC-Port-Binding, DHCP-Server-Screening, Safeguard Engine und die Unterstützung von Microsoft NAP einen wichtigen Baustein zur Bildung eines Gesamtkonzepts für Sicherheit, Stabilität, Performance, Redundanz und Verwaltbarkeit in Ihrem Netzwerk.

Whitepaper: Loopback Detection (LBD)

Aktuelle Themen im Rahmen					
Sicherheit	Stabilität	Performance	Redundanz	Verwaltbarkeit	D-Link Lösung
	Loop Connections				**Loopback-Detection**
	Mehrere DHCP Server				**DHCP Server Screening**
	Wurm Ausbrüche				**SafeguardEngine**
Wurm Ausbrüche					**Zonedefense**
ARP Spoofing					**IMPB v3**
Man in the Middle Attack					**IMPB v3**
Grundsätzlich geschützter Netzwerkzugriff					**ACL Liste Web based Access (WAC) 802.1x**
Erweiterter Netzwerkzugriff mit Policies					**Microsoft NAP**
		P2P Abusing			**Flow based Bandwidth Control**
			Chassis übergreifende Redundanz		**RERP (DES-7200)**
			Stacking		**Stacking auch über Glasfaser**
		Bandbreiten-erhöhung			**Stacking**
Überwachung / Konfigurations-rollout	Überwachung	Überwachung	Überwachung / Konfiguration	Einfache Administration	**D-View 6**

Folgende Switch Serien unterstützen Loopback-Detection:

- **DES-3010/18/26**
- **DGS-3200**
- **DES-3028/52**
- **DGS-3400**
- **DES-3528/52**
- **DGS-3600**
- **DES-3800**
- **DGS-3100**