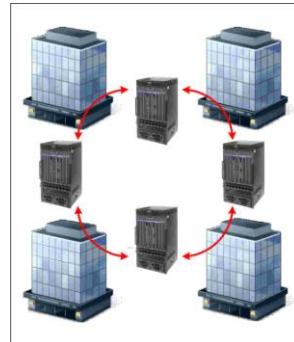


Whitepaper: Rapid Ethernet Ring Protection

Wenn Firmen in einer Campus ähnlichen Struktur über eine gewisse Fläche räumlich verteilt sind, oder mehrere Gebäude zu einem Firmenkomples miteinander verbunden werden sollen, so kommt netzwerktechnisch ein sogenannter Backbone zum Einsatz. Dieser ist von zentraler Bedeutung für das Netzwerk und muss damit hohen Ansprüchen genügen. D-Link hat das Protokoll RERP (Rapid Ethernet Ring Protection) entwickelt, damit der Backbone diesen hohen Anforderungen gerecht werden kann. Es ermöglicht redundante Strukturen, erkennt Ausfälle aktiver Verbindungen oder Geräte und schaltet blitzschnell um.

Der Backbone beinhaltet zum einen die notwendigen Verbindungen zwischen den einzelnen Standorten bzw. Gebäuden. Zum anderen sind hier die aktiven Netzwerkkomponenten angesiedelt, welche die Schnittstellen zu den einzelnen Gebäudenetzen bilden.

Als Verbindungen zwischen den einzelnen Standorten dienen unterschiedliche Glasfaserverbindungen, je nachdem welche Distanz überwunden werden soll. Kürzere Verbindungen bis ca. 550 Meter sind mit Multimode Glasfaserkabeln möglich. Für größere Distanzen werden Singlemode Kabel benötigt, welche das Lichtsignal weniger dämpfen. Parallel hierzu müssen auf Seiten der aktiven Komponenten die jeweils passenden Glasfaser Transceiver (z.B. SFP- oder XFP-GBICs) eingesetzt werden, die für Multi- oder Singlemode Verbindung verfügbar sind und, je nach Typ und Laser, Distanzen bis 80 Kilometer unterstützen.



Die Schnittstellen zu den Anwendern in den einzelnen Gebäuden bilden Netzwerkkomponenten wie zum Beispiel Gigabit Ethernet Switches. Sie stellen den Anschlusspunkt für die im Gebäude aufgebaute IT-Infrastruktur dar und bilden den Übergang vom Backbone in die einzelnen Netzwerksegmente.

Als zentrale und wichtige Stelle im Netzwerk ist der Backbone zugleich eine Art Achillessehne für Anwendungen und Daten. Fallen zentrale Komponenten wie Glasfaserverbindungen oder Switches innerhalb des Backbones aus, so werden die über das Netzwerk laufenden Applikationen empfindlich gestört. So können z.B. Datensicherungen abbrechen, Applikationen verzögert oder gar nicht mehr betrieben werden und, soweit bereits im Netzwerk implementiert, Telefonie über IP (VoIP) zusammenbrechen. Somit muss ein Backbone Redundanzen wie zum Beispiel gedoppelte LWL-Strecken oder Switches enthalten. Fällt eine Komponente während des Betriebs aus, springt das redundante Gegenstück ein und der Datenverkehr kann weiterlaufen.

Redundanzen im Netzwerk

Da Backbones typischerweise mit Hilfe von Ethernet (ein oder mehrmals Gigabit bzw. 10-Gigabit-Ethernet) realisiert werden, muss beim Einsatz von redundanten Switches und/oder Verbindungen verhindert werden, dass sich Schleifen, sogenannte Loops im Netz bilden. Hierfür findet im Normalfall das Spanning Tree Protokoll Anwendung. Dieses schaltet redundante Strecken bei Bedarf ein, wenn eine der Hauptstrecken ausgefallen sein sollte.

Im ungünstigsten Fall kann hierbei bei Standard Spanning Tree nach 802.1D eine Zeit zwischen 30 Sekunden bis zu über einer Minute vergehen, bis die Umschaltung erfolgt ist. Mit der Einführung von Rapid Spanning Tree (RSTP nach 802.1w) wurde diese Zeit auf ca. 1 Sekunde verkürzt.

Zeitkritische Anwendungen wie Citrix oder Realtime Applikationen wie IP-Telefonie oder Video Broadcasting reagieren aber auch bereits bei Ausfällen von einer Sekunde sehr empfindlich. Unter Umständen stürzen Citrix-Sessions ab und Telefonate erfahren Aussetzer oder brechen ganz zusammen.

Schnelle Reaktion gefordert - RERP

Um diesen hohen Anforderungen im Backbone gerecht zu werden, hat D-Link das **Rapid Ethernet Ring Protection** Protokoll entwickelt. Es verhindert, genau wie Spanning Tree auch, Schleifen im Netzwerk und erkennt Ausfälle von aktiven Verbindungen. Dabei schaltet es aber in bis zu 50 ms (0,05 Sekunden) um und erreicht so einen Wert, der auch für zeitkritische Anwendungen zu verkräften ist.

Whitepaper: Rapid Ethernet Ring Protection

RERP unterscheidet sich generell von der Funktionsweise von (Rapid) Spanning Tree. Bei diesem zentralisierten Protokoll übernimmt eine zentrale Komponente, der sogenannte Master, die Steuerung und Aktivitäten, während im Spanning Tree unterschiedliche Komponenten unterschiedliche Rollen bzw. Aktivitäten wahrnehmen. RERP ist ausschließlich in einer Ringstruktur einsetzbar und für Gigabit und 10-Gigabit Ethernet Strecken konzipiert, während Spanning Tree in den unterschiedlichsten Strukturen mit verschiedenen Link-Typen eingesetzt werden kann.

Dank der Spezialisierung auf eine ringförmige Backbonestruktur konnten die Konvergenzzeiten auf 30-50 Millisekunden reduziert werden. Weiterhin lassen sich mehrere Ringe koppeln, so dass auch komplexere Backbone-Netzwerke von den schnellen Konvergenzzeiten profitieren können.

Die prägnantesten Unterschiede zwischen Spanning Tree und RERP sind in der nebenstehenden Tabelle aufgeführt.

Unterschiede von (R)STP und RERP			
	STP	RSTP	RERP
Konvergenzzeit	30-50s	1s	30-50ms
Mögliche Topologie	Beliebig	Beliebig	Ring
Unterstützte Link-Typen	Beliebig	Beliebig	1Gig / 10Gig
Prozess Mechanismus	Verteilt	Verteilt	Zentral

RERP en détail

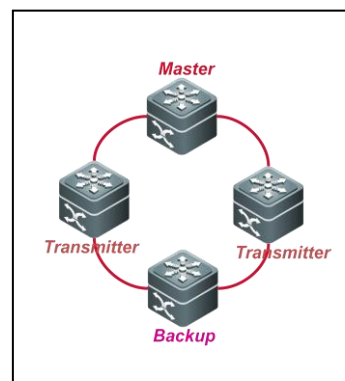
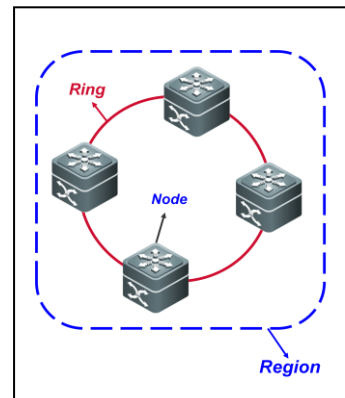
Der Aufbau von RERP beginnt bei der Definition einer Region mit einer dazugehörigen *Region_ID*. Dieser Region wird mindestens ein Ring zugeordnet, welcher über die *Ring_ID* spezifiziert wird. Die Switches (Nodes) schließlich, welche den Ring bilden, werden über die *Bridge_ID* identifiziert. Hierzu muss zusätzlich auf dem kompletten Ring ein dediziertes Control-VLAN eingerichtet werden, dessen Konfiguration untagged, also ohne 802.1Q Tag, erfolgt.

Zwar existieren bei RERP, wie auch bei Spanning Tree, unterschiedliche Rollen für unterschiedliche Geräte, allerdings wird bei RERP nur ein Gerät, der Master, auch wirklich aktiv, sollte eine Unterbrechung im Netzwerk identifiziert worden sein.

Doch zunächst zu den einzelnen Rollen, welche von den Switches innerhalb eines Backbone-Rings eingenommen werden können:

- **Master**
Der Master sendet die RERP-Kontrollpakete. Nur jeweils ein Switch pro Ring kann den Status eines Masters einnehmen. Der Ring wird vom Master unterbrochen, indem eines seiner Interfaces in den Status „Blocking“ geht und keinen normalen Datenverkehr mehr auf diesem Interface sendet.
- **Transmitter**
Die Switches im Status Transmitter hören auf die Kontrollpakete, welche vom Master gesendet werden. Außerdem melden sie diesem den Link Status ihrer Interfaces.
- **Backup**
Der Backup Modus ist ein spezieller Transmitter. Fällt der Master in einem Ring aus, so übernimmt der Switch im Modus „Backup“ dessen Status und ist ab diesem Zeitpunkt der neue Master.

Der *Master* Switch versendet in regelmäßigen Abständen Hello-Pakete von seinem aktiven Interface und führt darüber einen sogenannten „Robustness Check“ durch. Empfängt er die Hello-Pakete korrekt auf seinem zweiten Ring-Interface (welches sich für den normalen Anwenderdatenverkehr im Status „Blocking“ befindet), dann ist für ihn der Ring im Normalstatus.



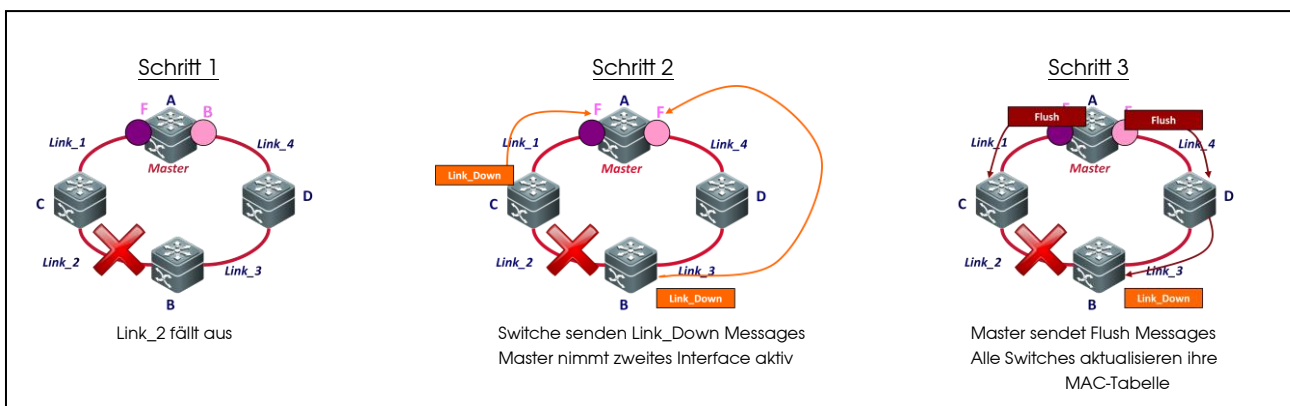
Whitepaper: Rapid Ethernet Ring Protection

Kommt es nun zu einer Unterbrechung des Rings, kann dies mehrere Ursachen haben:

- Eine Leitung des Rings wird unterbrochen
- Der Master Switch des RERP-Rings fällt aus
- Ein beliebiger anderer Switch (Node) innerhalb des Rings fällt aus

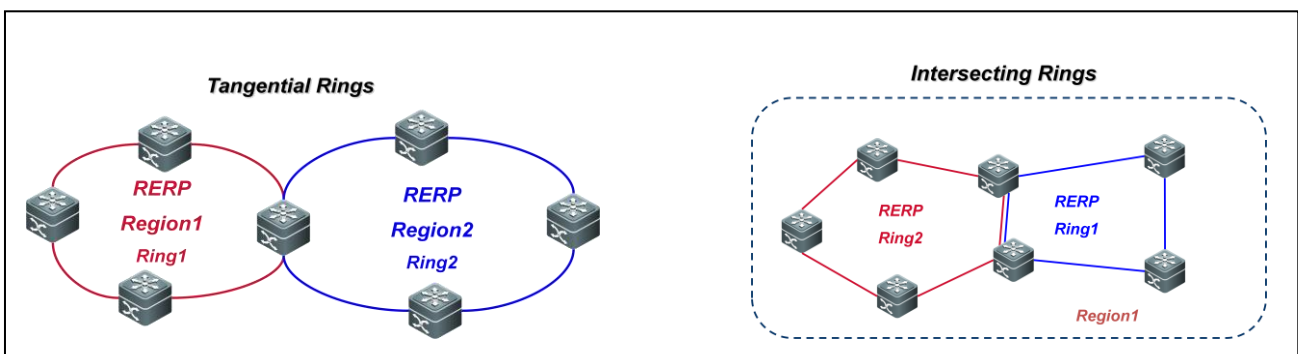
Fällt eine der Leitungen innerhalb des Rings aus, so unterscheiden sich die folgenden Schritte je nachdem, ob diese Leitung direkt am Master Switch oder zwischen anderen Switches innerhalb des Rings ausfällt. Ist der Link zwischen anderen Switches als dem Master ausgefallen, so senden die an diesen Link angeschlossenen Switches eine *Link_Down* Meldung in Richtung des Master Switches. Fällt der Link direkt am Master Switch aus, so kann dieser sofort aktiv werden, eine *Link_Down* Meldung wird nicht benötigt.

Bemerkt der Master Switch einen unterbrochenen Link, entweder direkt oder per *Link_Down* Meldung, so setzt er sofort sein zweites Interface, welches bislang im Status „Blocking“ war, in den Status „Forwarding“. Zusätzlich aktualisiert er seine MAC-Adress-Tabelle. Parallel dazu sendet er sogenannte „Flush“-Meldungen an alle Switches im Ring. Daraufhin aktualisieren auch diese Switches ihre MAC-Adress-Tabellen. Dies ermöglicht eine schnelle Wiedererreichbarkeit von Clients im gesamten Netzwerk.



Fällt direkt der Master Switch aus, so erkennt der Backup Switch dies anhand der dann ausbleibenden *Hello*-Meldungen. Hierbei zieht der *Fail_Timeout* Timer, welcher standardmäßig auf 3 Sekunden eingestellt ist. Der Backup Switch geht in den Status „Master“ und sendet nun seinerseits *Hello*-Nachrichten aus. Hierüber wird den anderen Switches im RERP-Ring bekannt, wer neuer Master im Ring ist. Ist der ehemalige Master Switch im Netz wieder verfügbar, so übernimmt er wieder seine Rolle und fängt an, *Hello*-Mitteilungen zu verschicken.

Von der Netzstruktur her ist nicht nur ein einfacher RERP-Ring möglich. Auch andere Strukturen sind realisierbar. Zum einen sind dies die sogenannten *Tangential Rings*, welche einen oder mehrere Switch(e) als Schnittpunkt haben und aus zwei unterschiedlichen Regionen bestehen. Zum anderen sind sogenannte *Intersecting Rings* möglich. Dort laufen zwei Ringe über eine gewisse Anzahl von Switchen parallel, gehören aber weiterhin einer gemeinsamen Region an.



Whitepaper: Rapid Ethernet Ring Protection

Die Konfiguration von RERP

Die Implementierung von RERP in einem Backbone erfordert eine gewisse Planung und eine schrittweise Konfiguration. Dabei sind die folgenden Schritte durchzuführen:

- Konfiguration von Trunks zwischen den einzelnen RERP Nodes (Switches)
Auf den Verbindungen zwischen den einzelnen Switches des RERP-Rings müssen die einzelnen VLANs konfiguriert werden. Zum einen sind dies die Daten-VLANs, welche als getaggttes VLAN eingerichtet werden müssen (über 802.1Q). Zum anderen ist es das Control-VLAN für RERP, welches als ungetaggttes (Port oder Native VLAN) konfiguriert werden muss.
- Einschalten von RERP auf den Switches
RERP muss global auf den einzelnen Switches aktiviert werden.
- Konfiguration der Region ID
Je nach benötigter Struktur des Backbones werden die Regionen eingerichtet, zu denen der Switch gehören soll. Bei einem einzelnen Ring oder bei *Intersecting Rings* erhalten die Switches jeweils eine *Region_ID*. Bei *Tangetial Rings* erhalten die Switches, welche die zwei Regionen miteinander verbinden, zwei *Regio_IDs* konfiguriert. Alle anderen erhalten ebenfalls eine *Region_ID*.
- Konfiguration der Rolle eines Switches
Nachdem RERP global eingerichtet wurde, wird im nächsten Step jedem Switch seine Rolle zugewiesen, entweder als *Master*, *Backup* oder *Transit Node*.
- Konfiguration des Control-VLAN auf den Switches und den Trunks
Als Control-VLAN muss ein VLAN gewählt werden, auf welchem kein VLAN-IP Interface (ein sogenanntes Switched Virtual Interface, kurz: SVI) konfiguriert wurde. Anderenfalls kann dieses VLAN nicht als Control-VLAN konfiguriert werden. Als Control-VLAN können die VLAN-IDs 2-4093 verwendet werden.
- Konfiguration der Port „Rolle“ (Active / Passive)
Jeder Switch in einem RERP-Ring erhält durch Konfiguration einen aktiven und einen passiven Port. Nur jeweils ein Port auf dem Switch, welcher nicht als Layer 3 Port oder als Teil einer Port Aggregation konfiguriert sein darf, kann als aktiver bzw. passiver Port konfiguriert werden.
- Konfiguration der Hello-Timer (Optional)
Das Zeitintervall, in welchem der Master Switch die Hello Pakete über den Ring sendet, kann im Bedarfsfall konfiguriert werden.
- Konfiguration der Fail-Timer (Optional)
Auch der Fail-Timer, welcher festlegt, wie lange ein Hello Paket ausbleiben darf, bis ein Master Switch seinen blocked Port aktiv nimmt, kann im Bedarfsfall konfiguriert werden.

Der Status der RERP Konfiguration und des Rings kann über „Show“-Kommandos überprüft werden. So bietet ein generelles „show rerp“ auf der Kommandozeile einen guten Überblick über die momentane Situation:

```
Des-7206#sh rerp
rerp state           : enable
rerp admin hello interval: 1(*1s)
rerp admin fail interval: 3(*1s)
rerp local bridge    : 00d0.f837.1930
-----
region 1
ring           : 1
rerp oper hello interval: 1
rerp oper fail interval: 3
ring master    : 00d0.f837.1930
ctrl-vlan      : 17
edge-vlan      :
role           : master
primary-port   : GigabitEthernet 0/23(forwarding)
secondary-port : GigabitEthernet 0/24(blocked)
```

Whitepaper: Rapid Ethernet Ring Protection

Zusammenfassung

Das D-Link Protokoll RERP ermöglicht die Realisierung redundanter Backbone Strukturen und ermöglicht Umschaltzeiten, die auch zeitkritische Anwendungen stabil halten und somit die Verfügbarkeit eines Backbone signifikant erhöhen.

RERP ist in den D-Link Switches der Serie DES-7200 verfügbar. Weitere Themen wie Sicherheit und Stabilität im Netzwerk, und wie diese mit Komponenten von D-Link in Ihr Netzwerk integriert werden können, sind in der nachstehenden Tabelle aufgeführt.

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