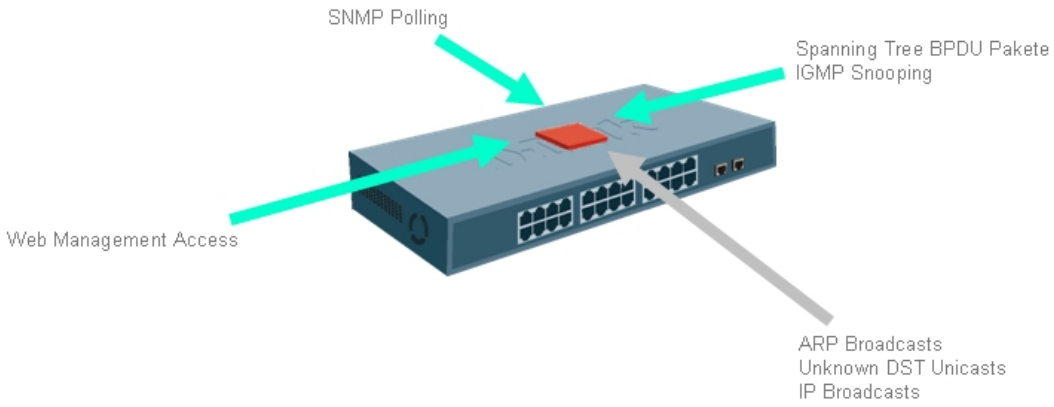
Whitepaper: SafeGuard Engine™

Mit der Einführung der Enterprise Produktlinie „xStack" hat D-Link dem Standard Feature Set managebarer Switches einige technologische Innovationen hinzugefügt. Diese übergreifende Eigenschaften xStack Produktfamilie stellen sicher, dass es sich bei der Vernetzung aktiver D-Link Komponenten um eine Lösung „aus einem Guss" handelt. Dazu gehören unter anderem das Single-IP-Management, IPv6 Unterstützung und die SafeGuard Engine.

Viele Komponenten einer lokalen Vernetzung zielen darauf ab, den ungestörten Betrieb bei hoher Leistung so lange wie möglich ununterbrochen aufrechtzuerhalten. Dazu gehören Vorkehrungen wie redundante Verbindungen, redundante Systeme und doppelte Netzteile, die aber nur den Hardwareausfall abfangen können. In jedem Switch wird ein erheblicher Teil der Kontrolle und Verwaltung durch die eingebaute Firmware erledigt, ohne die die Hardware nur ein Torso wäre. Um auch diesen Teil der aktiven Komponenten abzusichern, gibt es nützliche Software Funktionen, die dafür sorgen, dass unvorhersehbare Ereignisse nicht gleich das ganze Innenleben des Switches lahmlegen. Dafür sorgt eine weitere Funktionalität: Die **D-Link SafeGuard Engine™**.

CPU-gestützte Prozesse im Managed Switch

Im normalen Ethernet Datenstrom, der vom Switch einfach anhand der Zieladresse im Store-and-Forward Modus geprüft und weitergeleitet wird, finden sich immer wieder Pakete die eine schnelle Entscheidung durch die CPU erfordern. Dazu gehören zunächst Pakete wie SNMP und HTTP oder STP (Spanning Tree Protocol) die an die MAC-Adresse des Switches gerichtet sind. Sie dienen der Überwachung und der Konfiguration,und müssen entsprechend beantwortet werden. Andere Pakete werden nach Prüfung an einen oder mehrere Anschlüsse weitergeleitet, wie ARP-Anfragen, Multicast, IP-Broadcast sowie Pakete an unbekannte Adressen.



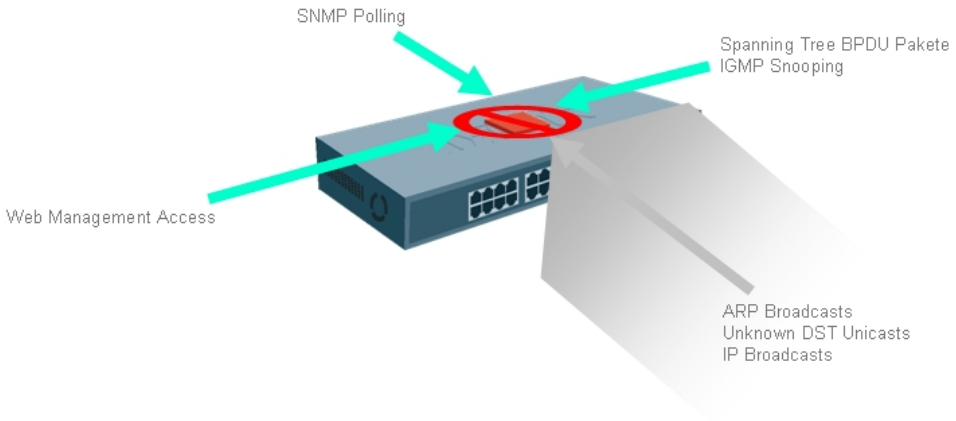
Der Anteil dieser Sonderaufgaben am gesamten Datenverkehr ist normalerweise eher gering.

Störung durch Virus- oder Wurmbefall: CPU Überflutung

Sind einzelne oder mehrere Stationen im lokalen Netzwerk durch Viren oder Würmer befallen, kann eine riesige Flut von CPU-Anfragen ausgelöst werden, die den Zugang zur CPU überlastet und regelrecht verstopft. In kürzester Zeit können solche Attacken den Switch komplett lahmlegen und alle bestehenden Verbindungen unterbrechen, so dass auch keine Gegenmaßnahmen durch Überwachung und Steuerung mehr möglich sind. Viren und Würmer erzeugen typischerweise große Mengen an CPU-intensivem Verkehr wie ARP-Broadcasts zur Verbreitung im Netz, so dass die Switch CPU in Mitleidenschaft gezogen wird.

D-Link®
Building Networks for People

Whitepaper: SafeGuard Engine™



Erst durch Einschalten der D-Link SafeGuard Engine wird die Switch CPU in die Lage versetzt, die Flutpakete zu drosseln und den notwendigen Teil der zur Verfügung stehenden CPU Bandbreite für die Überwachungs und Steuerungsfunktionen zu reservieren.

SafeGuard Engine™ Technologie

Die Bedrohung durch Paketüberflutung kommt aus dem eigenen lokalen Netzwerk. Dadurch ist eine Firewall am WAN-Zugang nur bedingt in der Lage, die Ausbreitung schädlicher Software zu verhindern, indem sie bekannte Bitmuster beim Empfang infizierter Daten erkennt und blockiert. Neue noch nicht bekannte Bedrohungen oder mitgebrachte Datenträger umgehen diesen Schutzwall unkontrolliert und können sich unbemerkt einnisten. Erst wenn sie sich selbst aktivieren, wird der Administrator den Netzwerkausfall bemerken und versuchen Gegenmaßnahmen zu ergreifen. Diese Arbeit wird erleichtert und beschleunigt, wenn die intelligenten Schaltstellen noch steuerbar sind. So kann der Ursprung der Flut schneller und leichter identifiziert und vom Netzwerk isoliert werden.

Ist die SafeGuard Engine in der Switchkonfiguration vorsorglich eingeschaltet worden, wirkt sie der Überflutung der CPU auf zwei unterschiedliche Arten entgegen:

Smart Managed Switch (2. Generation) SafeGuard Engine:

Der Zugang zur CPU des Switches wird in 4 Queues mit unterschiedlicher Priorität aufgespalten. Jede der 4 Queues wird in der Bandbreite so gedrosselt, dass nur noch ein fester Prozentsatz alller Arten von Paketen durchgelassen wird. So bleibt immer genügend Raum für das Switchmanagement, ohne dass bestimmte Arten von Datenverkehr komplett blockiert werden,

CPU Queue 0	Broadcast
CPU Queue 1	Smart Console Multicast
CPU Queue 2	„MAC-to-me" Unicast
CPU Queue 3	Anderer Traffic

Solange die SafeGuard Engine eingeschaltet ist, wird die Priorität der Pakete zur CPU immer definiert, auch wenn kein „Ernstfall" vorliegt. Die Queues 3, 2 und 1 haben Vorrang vor der Queue 0, in der sich die meisten Flutpakete sammeln. Die Werkseinstellung der SafeGuard Engine bei allen Smart Managed Switches der 2. Generation ist „aktiviert".

Managed Switch SafeGuard Engine:

Die SafeGuard Implementierung für die Managed Switch Serien ist etwas feiner und lässt sich darüber hinaus noch einstellen. Sobald die Engine aktiviert wird, werden zwei Bandbreiten-Begrenzungen gesetzt: Die erste für ARP-Pakete und

D-Link®
Building Networks for People

die zweite für IP-Broadcast Pakete. Für jede Begrenzung lässt sich ein oberer und unterer Schwellwert einstellen. Wenn die obere Schwelle mehr als 5 Sekunden lang überschritten wird, wird die jeweilige Bandbreiten-Begrenzung automatisch aktiviert und drückt den Anteil dieser Pakete unter die untere Schwelle. Nach weiteren 5 Sekunden wird die Begrenzung wieder aufgehoben. Wenn danach der obere Schwellwert gleich wieder für 5 Sekunden überschritten wird, wird die 2. Überlastschutz-Phase auf 10 Sekunden verdoppelt. Bei wiederholten Überflutungen wird die SafeGuard Aktionszeit immer weiter verdoppelt, bis maximal 320 Sekunden (5, 10, 20, 40, 80, 160, 320). Je nach Leistungsfähigkeit des Switch-Controllers kann die Begrenzung „strict" oder „fuzzy" ausgeführt werden. In der „strict" Variante werden die ARP- bzw. IP-Broadcast-Pakete komplett blockiert. Im „fuzzy" Betrieb wird immer noch ein automatisch bestimmter Anteil der Pakete zur CPU weitergeleitet.

Begrenzung der ARP-Pakete
- oberer und unterer Schwellwert, 20 – 100%
- fuzzy (automatisch)
- strict (blockiert)

Begrenzung der IP-Broadcast Pakete
- oberer und unterer Schwellwert, 20 - 100%
- fuzzy (automatisch)
- strict (blockiert)

SafeGuard Engine™ in der Praxis

Betroffene Switches bleiben trotz hoher Belastung managebar, bis der Administrator über das Netzwerkmanagement auch per Fernsteuerung für Abhilfe gesorgt hat. Ohne SafeGuard Engine hingegen wäre ein manueller Eingriff vor Ort oft unerlässlich.

Der „strict" Modus kann auch das Switch Management blockieren, und zwar solange, bis man die MAC-Adresse des Switches in der ARP-Cache des Management PCs eingetragen hat.

Layer3 Switches routen nicht mehr, wenn der Überlastschutz im „strict" Modus gerade aktiv ist. Hier geht es nur in den Zwischenzeiten weiter, wenn die Aktionszeit zu Ende ist.

Normale Pakete ohne CPU-Aufgabe werden vom Überlastschutz nicht beeinträchtigt

Stabilität und Verfügbarkeit im Netzwerk

Moderne Netze müssen performant, stabil und verfügbar sein. Gleichzeitig muss aber die Flexibilität und Ausbaufähigkeit gewährleistet sein. Die SafeGuard Engine bildet hierbei ein wichtiges Element, um Netzwerken diese Eigenschaften einzuräumen und gibt dem Administrator ein nützliches Werkzeug an die Hand, um Störungen schnell lokalisieren und eindämmen zu können, sowie um Netzwerke eine Störung schnell und dauerhaft automatisch einzudämmen.

Die SafeGuard Engine kann hierbei an unterschiedliche Szenarien angepasst werden und bietet dabei größtmögliche Flexibilität. Sie ist einfach einzurichten und ist in vielen unterschiedlichen Switches von D-Link verfügbar.

Sicherheitskonzept mit D-Link

Die D-Link SafeGuard Engine ist einer von mehreren Bausteinen für ein Netzwerk, das gleichermaßen Sicherheit, Stabilität, Performance, Redundanz und Verwaltbarkeit bietet. Zusammen mit weiteren hauptsächlich in xStack Switches

implementierten Funktionen, beispielsweise IP-MAC-Port-Binding, DHCP-Server-Screening, Loopback-Detection sowie die Unterstützung von Microsoft NAP bietet D-Link vielfältige Lösungen für Ihr Netzwerk.

Aktuelle Herausforderungen an Netzwerke und D-Link Lösungen					
Sicherheit	**Stabilität**	**Performance**	**Redundanz**	**Verwaltbarkeit**	**D-Link Lösung**
	Loop Connections				**Loopback-Detection**
	Mehrere DHCP Server				**DHCP Server Screening**
	Wurmausbrüche				**SafeGuard Engine**
Wurmausbrüche					**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 SafeGuard Engine:

- DES-1228/28P/52 (Smart II)

- DES-3028/52 **- DES-3526/50** **- DES-3528/52** **- DES-3800**

- DES-6500

- DGS-1224T/24TP/48 (Smart II)

- DGS-3100 **- DGS-3200** **- DGS-3400** **- DGS-3600**

- DES-7200 Chassis*

*** Zusatzinformation : Die Funktion Safe Guard Engine wird hier als CPU Protection Funktion (CPP) bezeichnet**

D-Link®
Building Networks for People