Managed Switch Solutions

D-Link Business Energizer

- Enhanced -

Christoph Becker

Senior Consultant
Business Development & Product Marketing

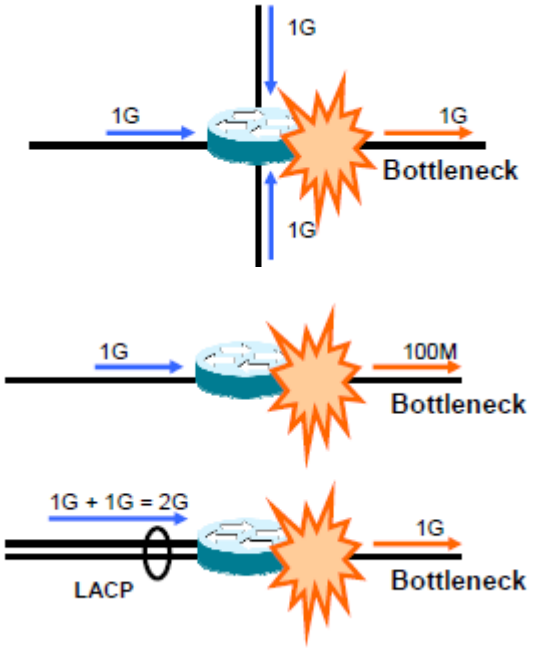
Inhalte des letzten Webinars

- Funktionsweise Switches
- Stack vs. Chassis
- Port Channels
- VLANs
- Spanning Tree
- Vorteile Managed Switche

QUALITY OF SERVICE

Quality of Service

- Ethernet an sich bietet seine Dienste nach dem „best efford“ Prinzip an
- Das bedeutet, dass Verkehr, so wie er am Switch / Router ankommt, verarbeitet wird
- Bandbreite ist hier nicht alles!
- Eine Priorisierung von Netzwerkverkehr wird notwendig
- Allerdings: QoS greift erst bei Überlastsituationen!

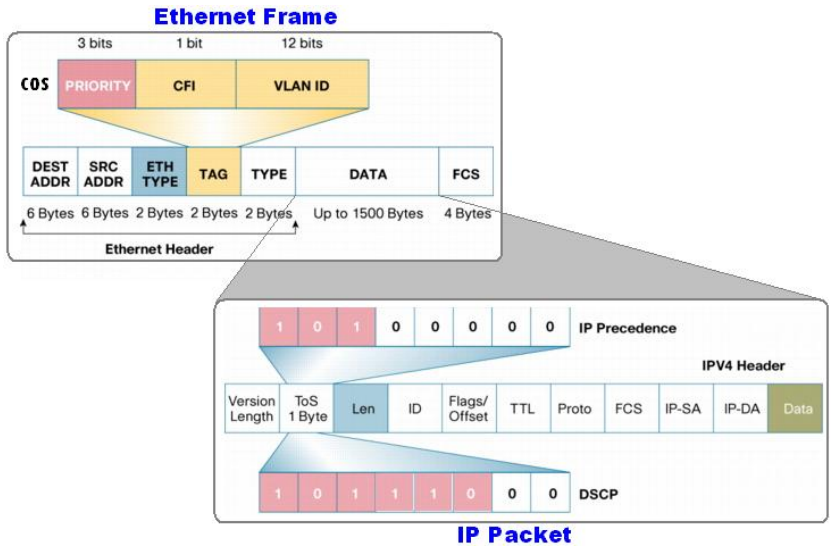


Quality of Service

- Geeignete Stellen im Netz zur Anwendung von QoS
  - Switchport
  - Zentraler Router/Switch
  - Übergang ins WAN
  - WLAN

- Integrierte Services (IntServ) vs. Differentiated Services (DiffServ)
  - RSVP (IntServ)
  - Class of Service (CoS) oder DSCP

- Markierung der Datenpakete
  - Layer 2 → 802.1p
  - Layer 3 → DSCP



Quality of Service

- Queues im Switch
  - Je nach Switchmodell (4 oder 8 Hardware-Queues)
- Markierung durch das Endgerät (Telefon o.ä.)
  - Geräte werden z.B. über VLAN Trunk an den Switch angeschlossen
  - Markierung (Taggen) der Sprachpakete im entsprechenden Voice-VLAN
- Remarking durch ACLs
  - Lässt der Netzwerkadministrator zu, dass „fremde" Geräte die Tags setzen?
  - Setzen der Tags durch den Switch (Access Control Listen) möglich
- Zuordnung der Queues
  - Standard-Queue pro Switchport definierbar
  - Zuordnung, welcher DSCP Wert welche Hardware-Queue nutzt

Die Verbindung von Netzen

ROUTING

Nötige Begriffe

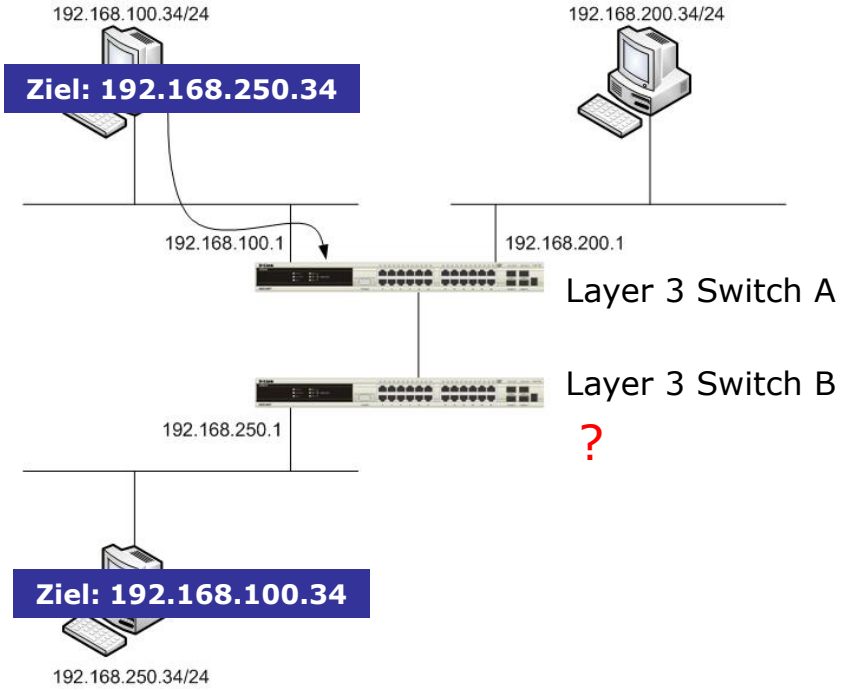
- Unicast
  - Datenpakete von einem Rechner zum anderen
- Broadcast
  - Datenpaket von einem Rechner an alle Rechner im gleichen Segment
- Multicast
  - Datenpaket von einem Rechner an mehrere Rechner in einem Netzwerk
- Routing
  - Leitet Netzwerkverkehr von einem Segment in ein anderes
- Layer 2 Netzwerk
  - Alle Teilnehmer befinden sich in im gleichen Netzwerksegment. Kein Routing. Alle Rechner haben IP-Adressen aus dem gleichen Subnetz. Unterscheidung nach MAC Adressen (OSI Layer 2 – „Data Link Layer" oder Sicherungsschicht)

Nötige Begriffe

- Layer 3
  - Bezeichnet des OSI Layer 3, den sogenannten „Network Layer" bzw. die Vermittlungsschicht. Auf dieser Ebene wird mit IP Adressen gearbeitet.
- Layer 2 Switch
  - Arbeitet ausschließlich mit MAC Adressen beim Transport von Datenpaketen. Unterstützt VLANs. Kann aber durchaus Access Listen anhand von IP-Adressen, TCP Ports und anderen Parametern verarbeiten. Routet NICHT!
- Layer 2+ Switch
  - Zusätzlich zum reinen Layer 2 Switch ermöglicht er statisches Routen zwischen IP-Segmenten (VLANs)
- Layer 3 Switch
  - Zusätzlich zum statischen Routen kann er Informationen, wo welche IP-Segmente zu finden sind, an andere Layer 3 Switche über ein dynamisches Routingprotokoll versenden (RIP, OSPF, BGP usw.)

Switch übergreifender Verkehr

- Zwei Möglichkeiten, Switch A die Netze von Switch B bekannt zu geben.
- Lösung 1: Statische Routen
- Switch A werden die Netze von Switch B manuall konfiguriert



Routing Tabelle Switch A

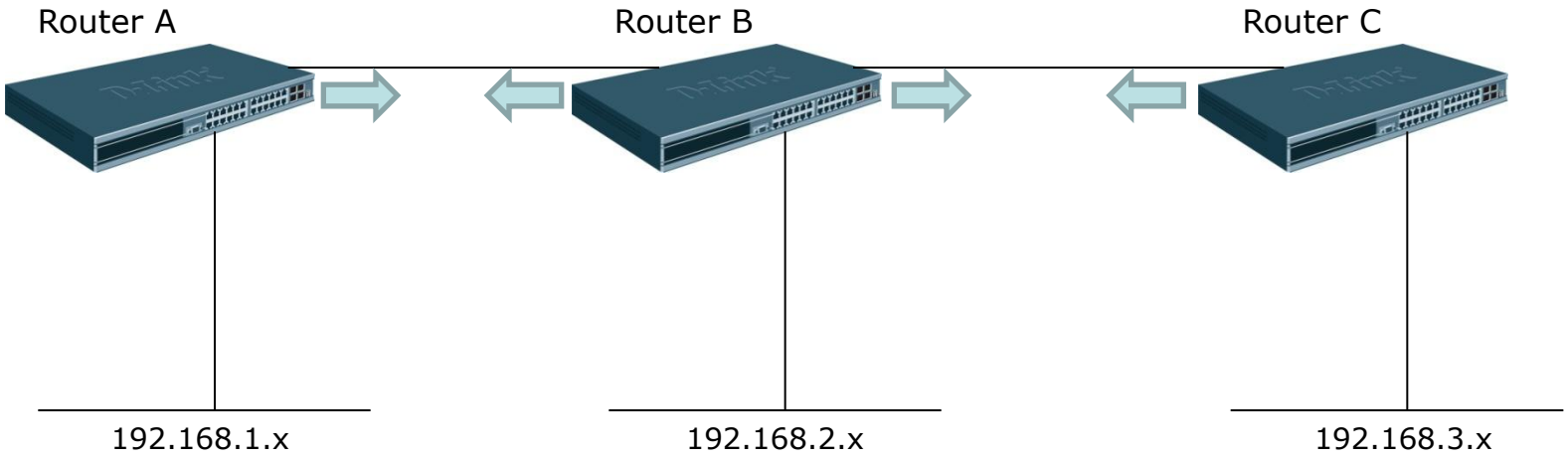
Zielnetz	Nexthop
192.168.250.0	Switch B

Routing Tabelle Switch B

Zielnetz	Nexthop
192.168.150.0	Switch A

Switch übergreifender Verkehr

- Dynamisches Routing
  - Automatische Wegefindung im Netzwerk mit RIP oder OSPF



Routingtabelle

Router	Netz
A	192.168.1.x
B	192.168.2.x
C	192.168.3.x

Router	Netz
B	192.168.2.x
A	192.168.1.x
C	192.168.3.x

Router	Netz
C	192.168.3.x
A	192.168.1.x
B	192.168.2.x

Dynamisches Routing

- Distance Vector (RIP, IGRP, EIGRP)
  - Jeder Router berechnet die Wege anhand eines Vektors, z.B. Anzahl Hops, Geschwindigkeit
  - Leitungsausfälle und / oder Änderungen im Netz brauchen Zeit, bis sie im ganzen Netz bekannt sind

- Link State (OSPF, ISIS)
  - Arbeitet mit SPF-Algorithmus (Shortest Path First)
  - Status des Nachbarn wird über ein Hello-Protokoll ermittelt
  - Regelmäßige Updates (nur die Änderungen werden übertragen)
  - Schnelle Reaktion auf Netzänderung: Der SPF-Algorithmus berechnet mit den LSA-Informationen die optimalen Pfade neu und aktualisiert die Routingtabelle (lokal)
  - Jeder Router hält eine komplette Linkstate Tabelle des Netzes vor, aus der er sich dann die für ihn gültige Routingtabelle errechnet

SICHERHEIT IM NETZ

Risiko offener Netzwerke

- Netzwerke bieten viele Möglichkeiten des ungewollten Zugriffs
  - Netzwerkanschlüsse in Besprechungsräumen
  - Ungenutzte Büros
  - Offene WLAN Access Points
  - Bewusste Angriffe durch ins Netzwerk eingebrachte Mini-Switche
- Die hierbei bestehenden Gefahren sind vielfältig
  - Mitschneiden des Datenverkehrs
  - Manipulation und Sabotage
  - Destabilisieren des Netzwerks durch falsch konfigurierte Rechner / Router

Zugang zum Netz beschränken

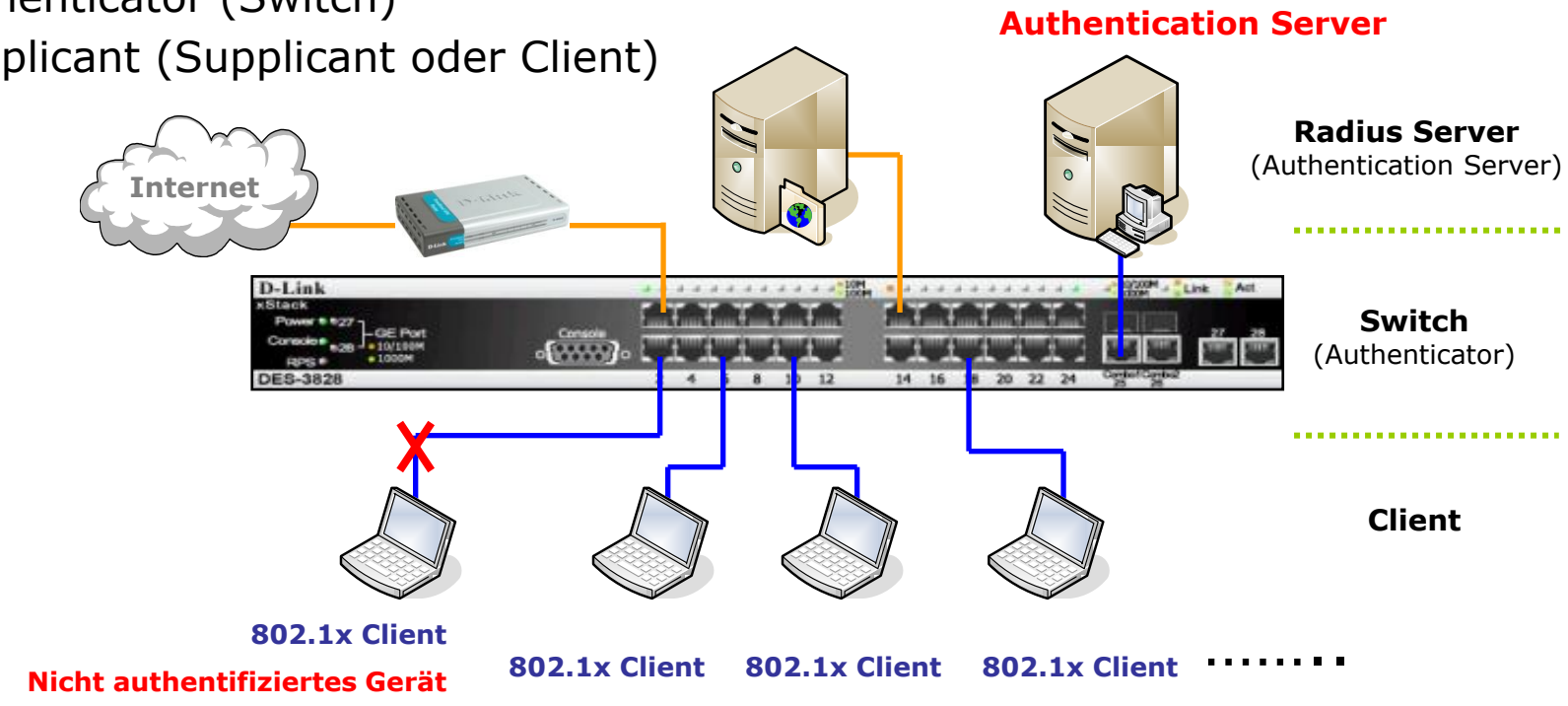
- Möglichkeiten, den Zugang zu einem Netzwerk zu beschränken, gibt es viele
  - Nur benötigte Netzwerkanschlusse auch am Switch belegen
  - Ungenutzte Switchports patchen, aber auf dem Switch in ein nicht geroutetes VLAN konfigurieren, welches auch nicht auf Inter-Switch-Verbindungen vorhanden ist.
- Vieles ist hierbei aber manuell
  - Konfigurationen müssen im Bedarfsfall durchgeführt werden
  - Konfigurationen für Gäste, z.B. in Besprechungsräumen, müssen später wieder rückgängig gemacht werden (zusätzliches Sicherheitsrisiko!)
  - Fehler sind sehr wahrscheinlich

→ Sicherheit mit einem Automatismus wird gesucht

Vorstellung von 802.1X

- Protokoll der IEEE
- Arbeitet mit folgenden Komponenten

  - Authentication Server (RADIUS Server)
  - Authenticator (Switch)
  - Supplicant (Supplicant oder Client)



Dynamische Parameter

- Über zusätzliche Parameter können bei der RADIUS Authentifizierung spezielle Konfigurationen im Switch durchgeführt werden
  - Zuweisung eines VLANs für den freigegebenen Switchport
  - Bandbreitenbeschränkungen
  - QoS Parameter
  - In zukünftigen Software Releases: Access Listen
- Eine manuell notwendige Konfiguration von Ports, z.B. in Besprechungsräumen, entfällt dadurch.
- Mobilen Rechnern mit installiertem VoIP Client können auf diese Weise z.B. die notwendigen QoS Parameter für den Anschlussport zugewiesen werden

802.1X Guest VLAN

- Für Anwender ohne gültige Authentifizierung bietet sich die Möglichkeit, in ein spezielles VLAN konfiguriert zu werden
- Das gibt dem Anwender Zugriff auf ein Netzwerk mit z.B. eingeschränkten Rechten wie Nutzung eines Druckers speziell für Besucher oder einen dedizierten Internetzugang
- Somit bleiben Gäste nicht vom Netzwerk ausgeschlossen sondern im Gegenteil bietet man ihnen einen speziellen Service

Gefahr: Instabil und unsicher

- Instabilitäten im Netzwerk
  - Applikationen sind nicht funktionsfähig – Verpasste Aufträge
  - Server sind nicht erreichbar – Keine Mail-Kommunikation
  - Über VoIP sind keine Anrufe mehr möglich
- Ursachen
  - Ungewollt / Unbewusst
  - „Mal ausprobiert“
  - Gezielte Angriffe und Störungen

Was gilt es wie zu schützen?

- Kombination von
  - MAC – Adresse
  - IP – Adresse
  - Switchport

  als Kriterium zur Überprüfung einer Manipulation

- IP-MAC-Port-Binding bietet diese Funktionalität und den daraus resultierenden Schutz des Netzwerkes vor ungewollten Veränderungen.

IP-MAC-Port-Binding (IMPB)

› Erklärung der Funktionsweise

- Durch IMPB entscheidet der Switch anhand einer gegebenen IP-MAC-Adressen Kombination, welche Ports welche Pakete empfangen dürfen.
- Alle Pakete werden verworfen, sollte deren Kombination aus IP- und MAC-Adresse sowie dem Switchport nicht exakt dem Eintrag in der „Adress-Binding-List“ entsprechen.
- Zwei unterschiedliche Modi, wie die Pakete überprüft werden, sind in dem Switch konfigurierbar

ARP-Mode und **ACL-Mode**

ARP-Mode vs. ACL-Mode

ARP Mode

- Überprüfung der eingehenden ARP Pakete
- Einfach zu konfigurieren und kein Einfluss auf Access-Listen

- Zu beachten:
  Ausschließlich „falsche“ ARP Pakete werden herausgefiltert

ACL Mode

- Überprüft den gesamten Verkehr
- Ist somit sicherer als der ARP Mode und filtert den gesamten schädlichen Verkehr

- Zu beachten:
  Verbraucht Access Listen. Generell muss die Konfiguration von ACLs berücksichtigt werden (Plausibilität)

IMPB mit DHCP-Snooping

DHCP-Snooping

- Bei der IMPB Konfiguration, sowohl im ARP als auch im ACL Mode, müssen die Eintragungen in der Address-Binding-List manuell eingetragen werden. Dies bedeutet einen erhöhten Betriebsaufwand bei größeren Netzen mit vielen Anwendern.

- Die Nutzung der DHCP-Snooping Funktion für IMBP ermöglicht den automatischen Aufbau der Address-Binding-List und vereinfacht somit den nötigen Konfigurationsaufwand.

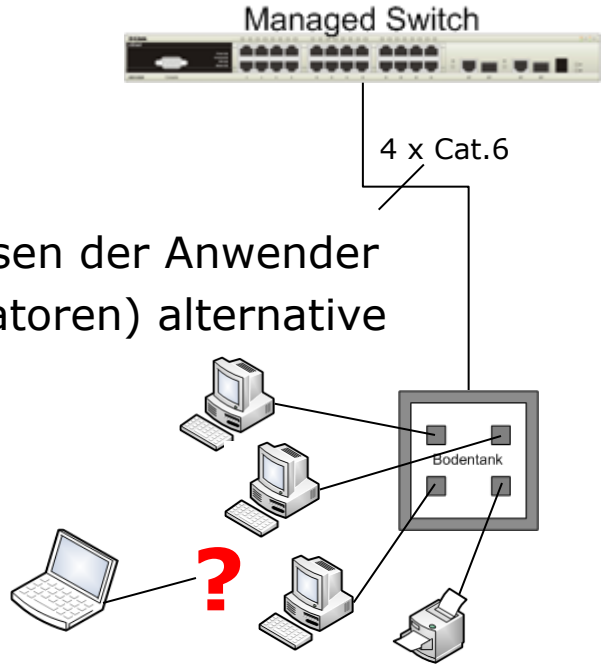
- Die Konfiguration von IMPB mit DHCP-Snooping „erzwingt" die Nutzung von DHCP auf den Clients. Clients mit statisch eingerichteten IP-Adressen erhalten keinen Zugriff auf das Netz.

LOOPBACK DETECTION

Strukturierte Umgebungen

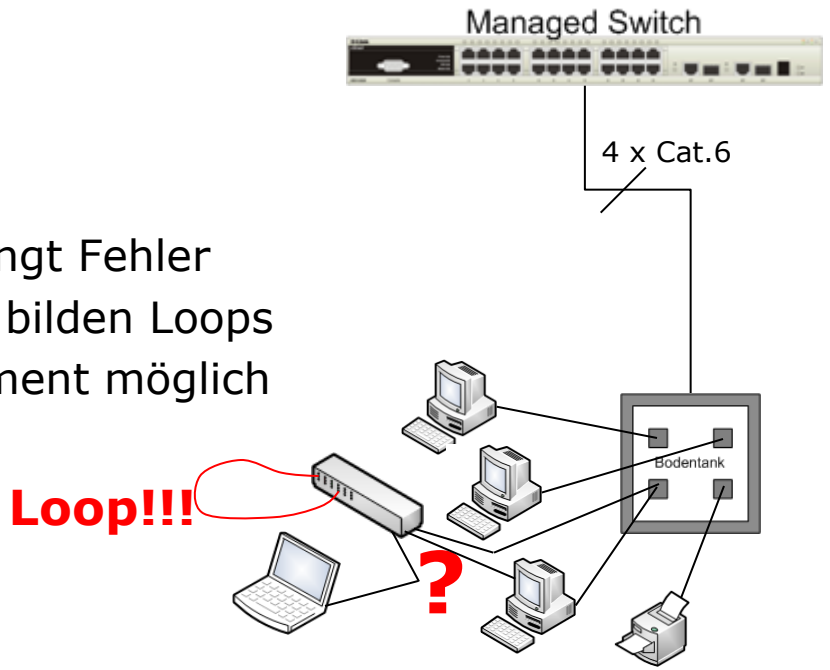
- Verkabelung in Büros und Gebäuden
  - Strukturierte Verkabelung bringt Ordnung ins Netzwerk
  - Eine Fehlersuche wird vereinfacht
  - Verwaltung der Geräteanschlüsse (PCs, Drucker, Faxgeräte)

- Aber
  - Eine fixe Verkabelung kann auch unflexibel sein
  - Sie wächst meist nicht so schnell wie die Bedürfnissen der Anwender
  - Bedingt, dass sich Anwender (oder auch Administratoren) alternative Lösungen suchen



Ideenreich und Erfinderisch

- Erweiterung in Büros oft problematisch
  - Anwender werden selbst aktiv
  - Hardware, die nicht im Firmenportfolio enthalten ist
  - Modifikationen vom Administrator oft nicht bemerkt
  - Neue Geräte nicht administrierbar
- Instabilitäten
  - Falsche oder fehlerhafte Verkabelung bringt Fehler
  - Aus Unwissenheit falsch gesteckte Kabel bilden Loops
  - Auswirkungen auf das gesamte Netzsegment möglich

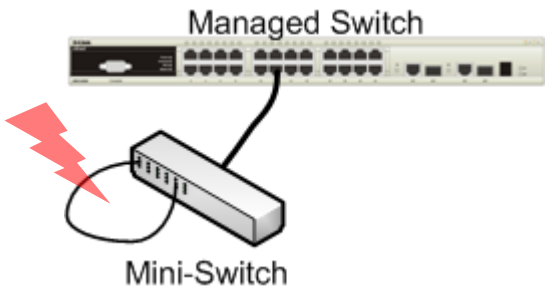


Loops trotz Spanning Tree

- Spanning Tree weist Grenzen auf
- Loops werde nicht erkannt, wenn sie hinter zusätzlich angeschlossenen Switches gesteckt werden und diese zusätzlichen Switche kein SPT sprechen
- Broadcast Loops auf diesen, zusätzlich angeschlossenen Switches bringen ebenfalls das gesamte Segment zum Stillstand

Lösung:

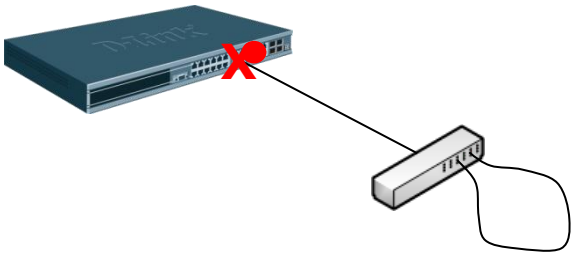
D-Link Loopback Detection



LBD Funktionsweise

- Unterschiede zwischen Version 2 und 4

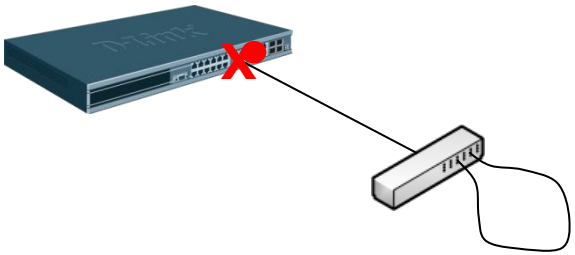
- Version 2
  - STP abhängig
  - Sendet zyklisch BPDU Pakete
  - Erkennt anhand dieser BPDUs am eigenen Port einen Loop und schaltet den Port ab



LBD Funktionsweise

- Unterschiede zwischen Version 2 und 4

- Version 4
  - Nicht abhängig von STP
  - Sendet zyklisch Multicast Pakete
  - Erkennt anhand dieser Multicasts am eigenen Port einen Loop und schaltet den Port ab

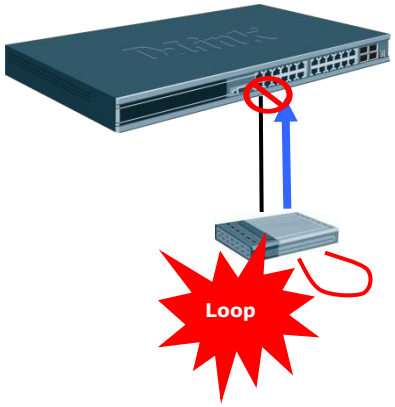


Port oder VLAN basierend

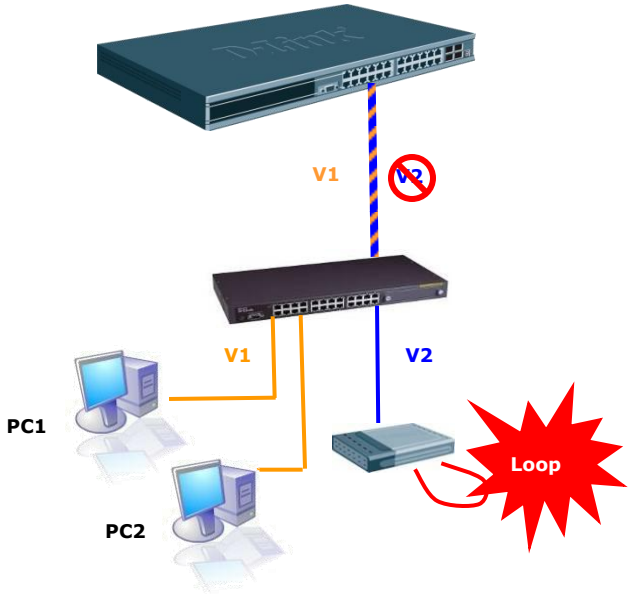
- Zwei Möglichkeiten der Konfiguration

  - **Port** basiert
    Wird ein Loop an einem Switchport erkannt, wird dieser komplett geblockt

  - **VLAN** basiert
    Nur das VLAN, in welchem der Loop ermittelt wurde, wird geblockt



1. Port basiert LBD

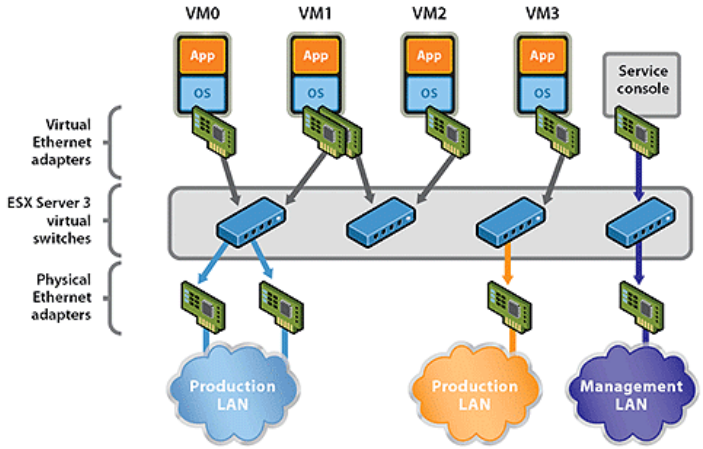


2. VLAN basiert LBD

ANBINDUNG VIRTUELLER WELTEN

Virtualisieren

- Momentan in aller Munde
- Wird als Grundlage für die „Cloud“ bezeichnet
- Alles – bin hin zum Switch – wird virtualisiert
- Das Netzwerk bekommt wieder eine größere Bedeutung im Rechenzentrum



Mehrere große Anbieter

- VM Ware
  - ESXi
- Microsoft
  - Hyper-V
- Citrix
  - Xen Server

Warum Virtualisieren?

› Software wird unabhängig von der Hardware

- Flexibler

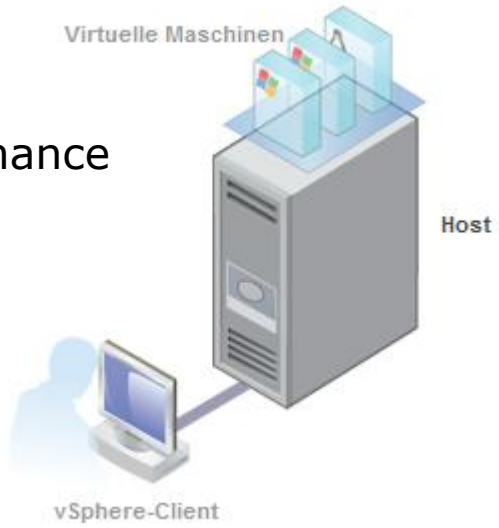
  - Verschieben von Servern auf neue Hardware möglich – ohne Neuinstallation und Neustart
  - Überlastsituationen können durch dynamisches Hinzuschalten zusätzlicher Server vermieden werden

- Schneller

  - Zusammenschalten von Servern steigern die Performance
  - Installation von tausenden Servern in kurzer Zeit

- Ausfallsicher

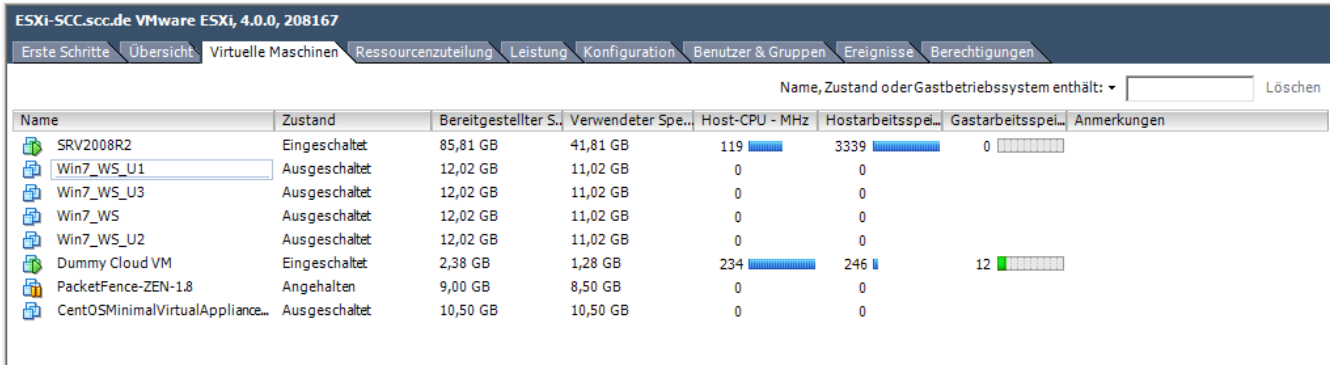
  - Variable Redundanzkonzepte



Was bedeutet Virtualisieren?

- Ein Rechner (der Host) wird mit einem Grundbetriebssystem und der Virtualisierungssoftware installiert

- In dieser Software werden die eigentlichen Server (sprich virtuelle Maschinen) installiert



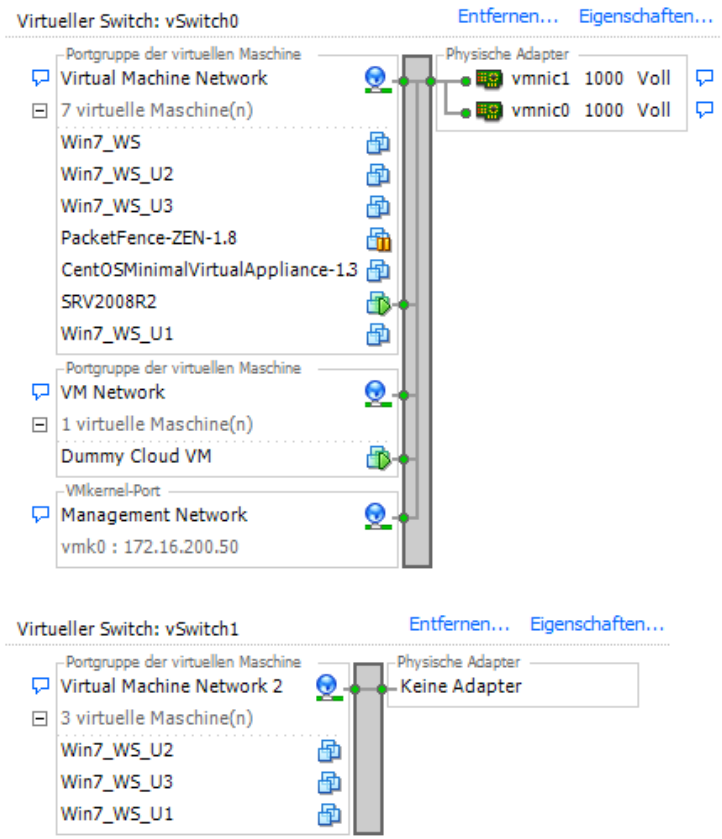
- Verwaltung über Client Software (z.B. vSphere Client) bzw. Management Systeme (z.B. vCenter Server)

Hardwareverwaltung

- Den Virtuellen Maschinen kann Hardware zugewiesen werden
  - Speicher
  - CPU Kerne
  - Netzwerkkarten
- Die zugewiesene Hardware wird dann im Virtuellen System als Hardware erkannt und kann konfiguriert werden
- Auch virtuelle Hardware ist hierbei möglich (z.B. Netzwerkkarten)

Virtuelle Switches

- Einer oder mehrere virtuelle Switch (vSwitch) in einem Host konfigurierbar
- Unterstützt VLANs und Trunking
- Flexible Konfigurationen denkbar
- Bilden die Verbindung in die reale Welt



Verbindung zu „realer“ Hardware

- Problemloser Anschluss an D-Link Komponenten
- Trunking ist statisch möglich (dynamisch via LACP unterstützt z.B. VM-Ware nicht)
- Auf Duplex und Speed Einstellungen achten!
- Die virtuellen Switches unterstützen kein Spanning Tree
- z.B. für VM-Ware ist ein Netzwerk Guide verfügbar

  http://www.vmware.com/files/pdf/virtual_networking_concepts.pdf

Vielen Dank für Ihre Teilnahme