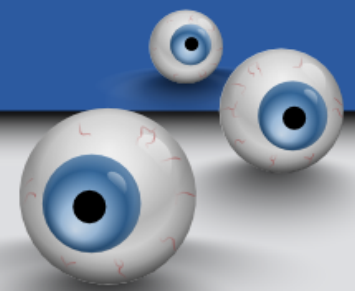
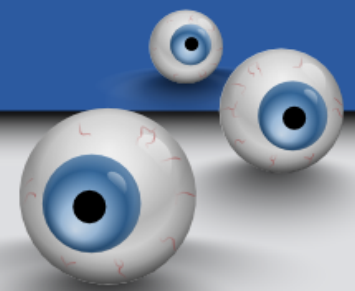


Ethernet: Sicherheit & Performance



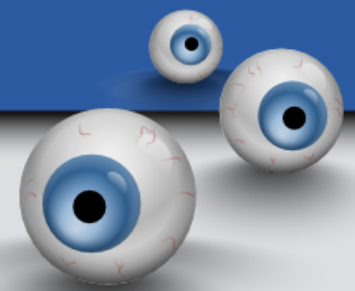
Agenda

- Was haben wir heute ?
- Welche neue Anforderungen haben wir ?
- Was folgt daraus ?
- Wie könnte eine Umsetzung aussehen ?



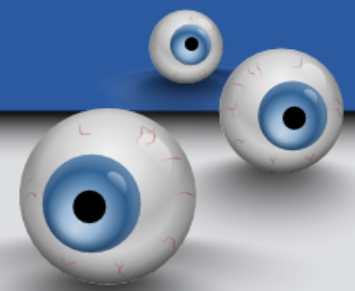
👁️ Was haben wir heute ?

- Ethernet als Transportnetz
- IP als Protokoll
- Lokaler Storage (Direct Attached Storage)
- Keine durchgängige Verschlüsselung
 - SSH ja, aber viele andere Tools nicht
 - Backup-Konsolen, Virusscanner-Konsolen, Nagios über HTTP, ...
- Lokales Netz nicht vertrauenswürdig



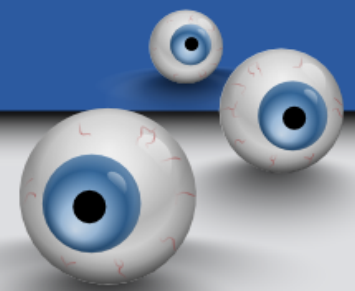
🕒 **Neue Anforderungen: Performance**

- Latenzen stabil runter für VoIP und Collaboration (interaktive Nutzung statt Fileserver)
- Storage wandert von DAS (SCSI und Fibre Channel) auf NAS (iSCSI und FcoE)
- Raum-, Gebäude- und Standort-übergreifende Layer 2 Netze für Cluster / FCoE
- Mehr Durchsatz für iSCSI und FcOE



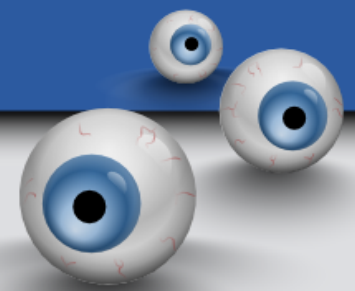
👁️ **Folgerungen: Performance**

- Überall 10 Gigabit Ethernet ?
 - Leider sehr teuer, kurze Kabel
 - Daher nur meistens für Storage
- Trennung von Datenströmen: Backup und SAN belasten das Netz sehr und treiben die Latenzen hoch, User-Verkehr teilweise sehr stoßweise
- Isolation der Anwendungen in Layer 2 Zonen, weil die Layer 2 Schicht sonst zu viele Systeme beinhaltet



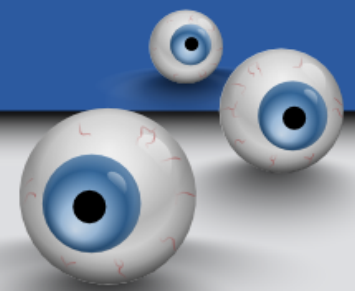
• **Neue Anforderungen: Sicherheit**

- Virtualisierung über Sicherheitszonen hinweg nicht immer zulässig
- Ist das eigene Netz vertrauenswürdig ?
- Verschlüsselung:
 - SAN (iSCSI ...) ist unverschlüsselt
 - FcoE ist kein IP, daher kein IPSec oder SSL
 - Auch Management-Tools
- Outsourcing / Offshore-Fähigkeit:
 - Kunden sicher einbinden
 - Outsourcer sicher einbinden
 - Isolation auf die beauftragte Anwendung



👁️ **Folgerungen: Sicherheit**

- VLANs aufheben, wenn unzulässig
- SAN (iSCSI ...) über IPsec ist eine Performance-Katastrophe: daher separieren
- FcoE: kein Crypto / Firewall, da kein IP
- Trennung der Datenströme
- Verschlüsselung auf Netzebene
 - Management-Tools können das teilweise nicht selber
 - Alte Tools im Einsatz



Architektur

- Trennung der Datenströme
 - Administration
 - User
 - Storage
 - Betrieb: Monitoring / Deployment / ...
- Administration über IPSec

