Netzdesign und Sicherheit

Switch-Einsatz im Schul-LAN

Themen:

- Dimensionierung der Bandbreiten
- Trennung durch VLAN und Firewall
- Management-VLAN
- Zugangs- und Zugriffsschutz
- Loop-Detection, redundanten Pfade
- Konfiguration sichern
- Port-basierte Sicherheit
- USV-Einsatz im Serverraum
- Dokumentation

Das Unterrichtsnetz bietet der schulischen Lerngemeinschaft einen funktionsstabilen und performanten Zugang zu digitalen Lernmitteln. Dieser Bedeutung gilt es hinsichtlich Netzdesign und Sicherheit Rechnung zu tragen. Sicherheit wird hier auch als Funktionssicherheit betrachtet.

Der pädagogische Bereich eines Schulnetzes ist besonderen Anforderungen ausgesetzt:
In kürzester Zeit meldet sich eine große Zahl an Nutzern an und greift auf interne oder externe Ressourcen zu. Funktionsstabile Netzwerke verkraften diese Lastsituationen und bieten stabile Bandbreiten.
Die Basis dafür sind, neben einer breitbandigen Verkabelung, die Netzwerk-Switches. Als Bereichsverteiler arbeiten Layer-2-Switches (L2) auf den Etagen oder im Klassenzimmer. Sie bieten den Endgeräten und Access-Points Zugang zum Schulnetz.
Ein zentraler Layer-3-Switch (L3, Routing-Switch) im Serverraum bildet zusammen mit den verteilten Switches das Rückgrat des Schulnetzes.

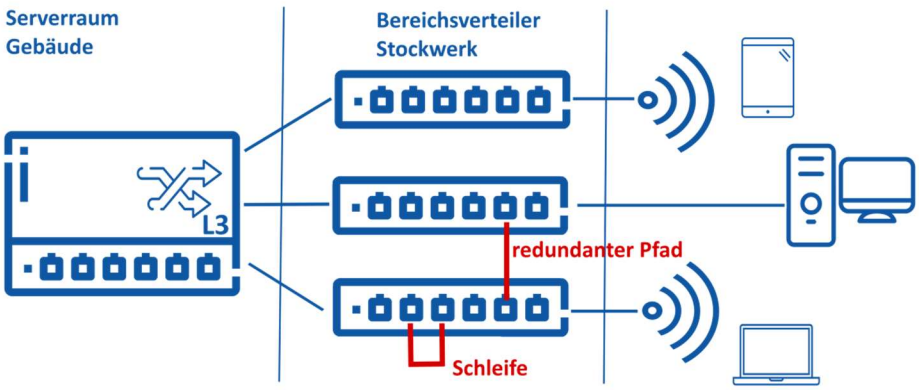
Während einfache Switches (L2) primär als Konzentratoren arbeiten, kommt dem zentralen L3-Switch die weitere Aufgabe des Routings und der Zugriffssteuerung zu.

Netzdesign

Lokale Netzwerke sind grundsätzlich in Sterntopologie aufgebaut. An einem zentralen Verteilerpunkt (meist L3-Switch) sind weitere Verteiler auf den Stockwerken angeschlossen. Die Anbindung sollte über Lichtwellenleiter erfolgen. Diese bieten skalierbare Bandbreiten, lange Installationsstrecken und eliminieren unerwünschte Nebeneffekte.
Redundante Switching-Pfade erhöhen bei Bedarf die Ausfallsicherheit von Übertragungsstrecken. Diese erfordern den Einsatz des Spanning-Tree-Protokolls mit entsprechender Konfiguration. In Schulnetzen sind redundante Pfade in aller Regel nicht erforderlich.

Störgrößen

Gebrückte Switchports führen zur Schleifenbildung (Loops). Ein falsch gestecktes Netzwerkkabel ist häufig ein Grund dafür. Der physische Zugang zu Switches sollte nur autorisierten Personen (Systembetreuung) möglich sein. Ein Loop kann so nur an den zugänglichen Netzwerkdosen gesteckt werden und ist meist leicht lokalisierbar.

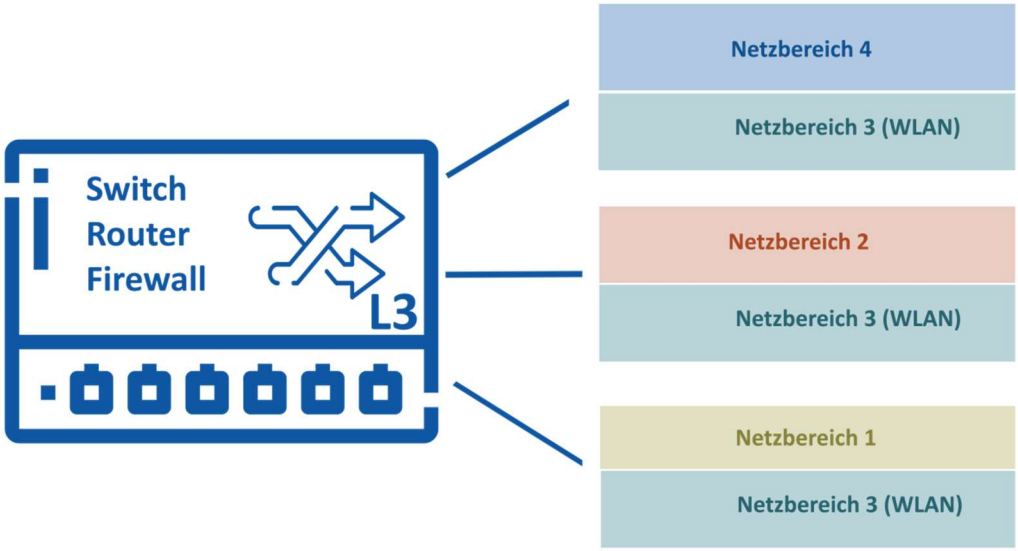


Schleifen können einen Switch oder auch ein ganzes Netzwerk zum Absturz bringen. Die Funktion Loop-Detection oder das Spanning-Tree-Protokoll des Switches kompensieren solche Beeinträchtigungen unter der Voraussetzung, dass das Switch-Modell dies unterstützt.

Die Funktionsstabilität kann durch weitere Aspekte beeinträchtigt sein. Schon die falsche Dimensionierung der Datenübertragungsrate kann zu Fehlfunktionen führen. Die Kalkulation der benötigten Bandbreite steht deshalb zu Beginn jeder Planung.
Ein kurzzeitiger Stromausfall im Serverraum wird durch den Einsatz einer „Unterbrechungsfreien Stromversorgung“ (USV) aufgefangen. Für Switches im Bereichsverteiler (Stockwerk/Klassenzimmer) des pädagogischen Netzwerks ist das in aller Regel nicht notwendig.

Segmentierung durch virtuelle Netze (VLAN)

Mit geeigneten konfigurierbaren Switches ist es möglich, ein Netzwerk in logische Teilnetze (VLAN)aufzuteilen. Die Kommunikation zwischen verschiedenen VLANs ist nur über den L3-Switch bzw. einen Router möglich. Die Firewall auf dem L3-Gerät steuert die Inter-VLAN-Kommunikation. Mit VLANs lassen sich bereits auf Netzwerkebene sicherheitsrelevante Netzbereiche, beispielsweise ein Unterrichtsnetz und ein Lehrernetz, abtrennen.
Eine Aufteilung in verschiedene Gebäudebereiche ist ebenso möglich. Diese Maßnahmen erhöhen die Funktionsstabilität sowohl der Teilbereiche als auch des gesamten Schulnetzes.



Netzwerkgeräte: Zugang und Zugriff

Der physische Zugang zu einem Switch ist einzuschränken. Abschließbare Netzwerkschränke bieten dafür den notwendigen Schutz. Ebenso ist der Serverraum nur für autorisiertes Personal zugänglich.

Die Konfiguration des Switches darf nur durch die Systembetreuung, den Schulaufwandsträger oder Beauftragte erfolgen. Ein Passwort schützt vor unberechtigtem Zugriff. Differenzierte Zugangslevel können die Konfiguration oder z.B. nur das Monitoring ermöglichen.
Der Zugang über das Netzwerk kann durch entsprechende Netzwerkkonfiguration weiter eingeschränkt werden. Ist das Netzwerk durch virtuelle Teilnetze (VLAN) strukturiert, werden die Switches einem separaten „Managementnetz“ zugeordnet. Der Zugriff aus dem VLAN „Unterrichtsnetz“ sollte nicht erlaubt sein.

Erweiterte Sicherheit, NAC

Port-basierte Sicherheit bietet ein zusätzliches Maß an Zugriffsschutz. So kann festgelegt werden, welches Endgerät mit welcher MAC-Adresse an einem definierten Switch-Port angeschlossen werden darf.
Ein höheres Maß an Zugangssicherheit biete Network-Access-Control (NAC). Dieses Konzept erfordert eine Authentifizierung und ermöglicht einen personen- bzw. rollenbasierten Zugang zu definierten Netzbereichen.
Die funktionell pädagogische Ausrichtung eines Schulnetzwerks und der hohe Administrationsaufwand rechtfertigen den Einsatz dieser Maßnahmen in aller Regel nicht.

Logging und Monitoring

Bewegungen im Netzwerk bzw. Zugriffe lassen sich, je nach Switch-Modell, aufzeichnen. Systemlogs können technische Merkmale wie Auslastung oder Fehlerfälle protokollieren.
Spezielle Monitoring-Funktionen lassen ggf. auch den Mitschnitt von Nutzdaten zu. Aus datenschutzrechtlichen Gründen bedarf es für diesen Einzelfall der Speicherung und Auswertung einer berechtigten Anordnung. Im Schulumfeld dürfte es hierfür kaum Anlass geben.

Konfiguration

Konfigurationsdateien der Switches sind an einem sicheren Speicherort abzulegen. Der Zugriff darauf ist nur von autorisiertem Personal möglich.