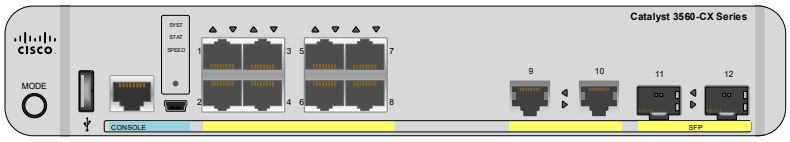
Infoblatt:

Pädagogisches Netzwerk Schulen-SH

(GBG037 im LNSH)

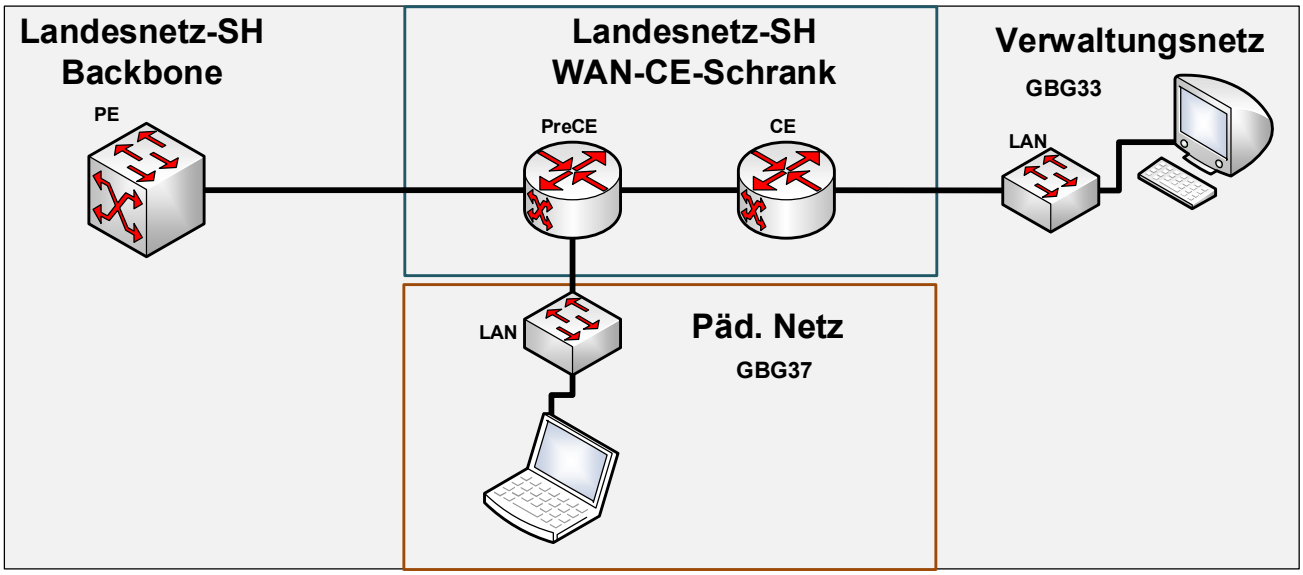


Inhalt

1. Allgemeines: 2
2. Physikalischer Aufbau vor Ort in der Schule 3
3. IPv4-Netz-Aufbau 4
4. WLAN 5
5. Sicherheitspolicy 6
6. URL-Filter 7
7. FAQ 8

1. Allgemeines:

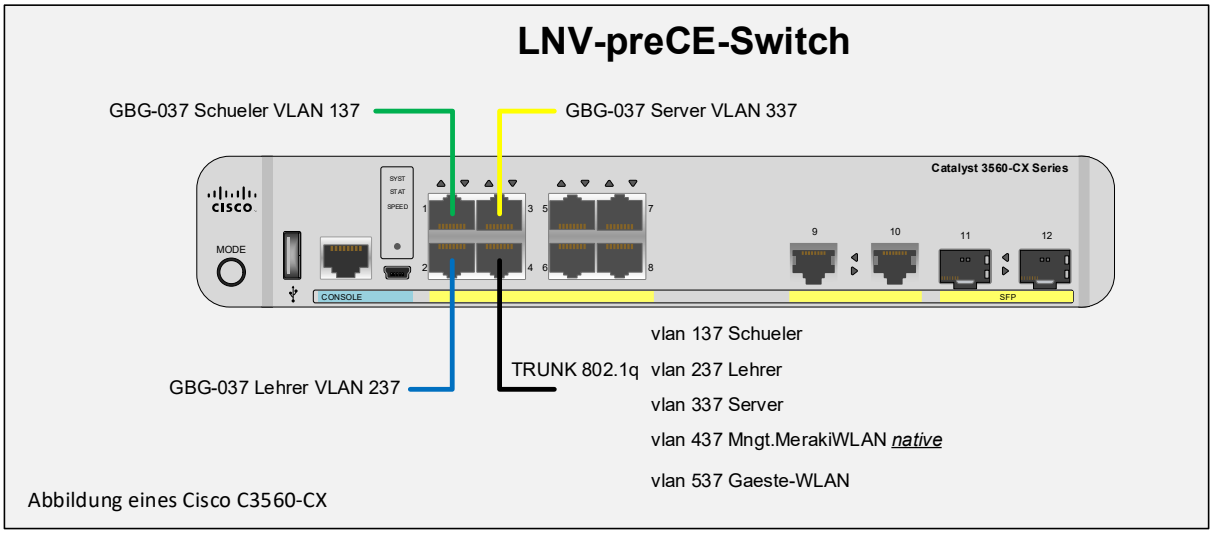
Das folgende Infoblatt enthält die wichtigsten Hinweise für den pädagogischen Internetzugang der Schulen in Schleswig-Holstein. Für das pädagogische Netz wurde im Landesnetz SH eine geschlossene Benutzergruppe eingerichtet (GBG037), die durch das WAN transportiert wird. Das lokale Netzwerk in der Schule ist nicht Bestandteil dieser Betrachtung und kann in eigener Verantwortung betrieben werden.



Netzplan zum Anschluss des Schüler- und Verwaltungsnetzes in der Schule

2. Physikalischer Aufbau vor Ort in der Schule

Der Einbau der Netzwerkkomponenten Landesnetz-SH erfolgt in der Schule in den verschlossenen Landesnetz-Schrank. Die Schulen erhalten keinen Zugriff auf die dort verbauten Komponenten. Im Landesnetz-Schrank ist ein LNV-CE-Router für das Verwaltungsnetz sowie ein LNV-preCE-Switch verbaut, über den das pädagogische Netzwerk bereitgestellt wird. Die farbigen Verbindungskabel werden bei der Installation aus dem Schrank geführt.



Das Schüler-Segment wird im Normalfall im VLAN 137 am Port 1 (grünes Netzwerkkabel) bereitgestellt. IP Adressen werden per DHCP mit der Netzwerkmaske 255.255.254.0 zugewiesen. Die IP Adressen 10.x.x.1-15 sind den Dataport-WAN-Komponenten vorbehalten.

Das Lehrer-Segment wird im Normalfall im VLAN 237 am Port 2 (blaues Netzwerkkabel) bereitgestellt. IP Adressen werden per DHCP mit der Netzwerkmaske 255.255.255.0 zugewiesen. Die IP Adressen 10.x.x.1-15 sind den Dataport-WAN-Komponenten vorbehalten.

Das Server-Segment wird im Normalfall im VLAN 337 am Port 3 (gelbes Netzwerkkabel) bereitgestellt. IP Adressen müssen alle statisch vergeben werden, Netzwerkmaske 255.255.255.0-Die IP Adressen 10.x.x.1-15 sind den Dataport-WAN-Komponenten vorbehalten.

Am Port 4 (**schwarzes Netzwerkkabel**) werden im Normalfall die verschiedenen VLANs über einen Trunk übergeben. Hierbei werden die verschiedenen VLANs über eine Verbindung getagged (IEEE 802.1Q) übertragen.

Die vorgegebenen VLAN-IDs sind bindend und dürfen in der Schule nicht anderweitig verwendet werden.

3. IPv4-Netz-Aufbau

Jede Schule bekommt für die verschiedenen Netze einen eigenen Bereich zugewiesen.

Angeschlossene Clients (außer Servernetz) bekommen per DHCP automatisch eine IP-Adresse aus dem zugeteilten Netz sowie die DNS-Server und das entsprechende Gateway zugewiesen.

Die Adressen 10.x.x.1 - .15 sind den Dataport-WAN-Netzwerkkomponenten vorbehalten und dürfen nicht anderweitig vergeben werden.

Die IP-Adresse 10.x.x.1 dient als Default-Gateway.

Die Adressen 10.x.x.16 - .31 können von der Schule statisch an Komponenten vergeben werden.

Die Adressen 10.x.x.32 – 10.x.x.254 werden automatisch per DHCP vergeben. Eine Ausnahme stellt hier das Servernetz dar, dort müssen alle Adressen statisch vergeben werden.

Als DNS-Server wird 10.65.104.245 (Backup 9.9.9.9) per DHCP an die Clients übermittelt.

Für Endgeräte, denen statische IP-Adressen zugewiesen werden, müssen DNS-Server und Gateway ggf. manuell auf den Clients konfiguriert werden.

Das weitere Netzdesign hinter dem preCE obliegt der Schule. Eine weitere Unterteilung bzw. eine Vergrößerung des Netzbereiches kann z.B. durch einen, durch die Schule eigenverantworteten, PAT-Router erreicht werden.

10.72.x.x	Schülernetze
10.73.x.x	Schülernetze
10.74.x.x	Schülernetze
10.75.x.x	Schülernetze
10.76.x.x	Schülernetze
10.77.x.x	Schülernetze
10.78.x.x	Schülernetze
10.79.x.x	Schülernetze
10.80.x.x	Lehrernetze
10.81.x.x	Lehrernetze
10.82.x.x	Lehrernetze
10.83.x.x	Lehrernetze
10.84.x.x	Servernetze
10.85.x.x	Servernetze
10.86.x.x	Servernetze
10.87.x.x	Servernetze
10.88.x.x	Meraki-Mngt
10.89.x.x	Meraki-Mngt
10.90.x.x	Meraki-Mngt
10.91.x.x	Meraki-Mngt
10.92.x.x	Gäste
10.93.x.x	Gäste

4. WLAN

WLAN kann Optional dazu gebucht werden. WLAN steht für Wireless Local Area Network und ist ein kabelloses Netzwerk, das Ihnen ermöglicht Endgeräte flexibel in Ihrer Schule einzusetzen und mobilen Endgeräten einen Zugriff auf das Netzwerk oder das Internet zu öffnen.
Für die Bereitstellung der dSchul-WLAN Lösung an Ihrer Schule sind sogenannte Access Points notwendig, welche gesondert über Dataport beauftragt werden müssen.

Die Access Points müssen an Port 4 des preCE-Switches angeschlossen werden (schwarzes Netzwerkkabel).

Folgende SSIDs werden über das optionale WLAN zur Verfügung gestellt:

SSID	Verwendung	Zugangsmöglichkeit
dSchueler	WLAN für die Schüler	Zugang per PreShared Key oder schuleigene RADIUS Infrastruktur
dLehrer	WLAN für die Lehrer	Zugang per PreShared Key oder schuleigene RADIUS Infrastruktur
dGaeste	WLAN für Gäste	Zeitlich befristeter Zugang über Sponsor Portal

Für die SSIDs gelten die unter Punkt 5 beschriebenen Zugriffsmöglichkeiten.

5. Sicherheitspolicy

Die verschiedenen lokalen Netzwerksegmente werden durch Access-Listen gegen Zugriffe aus den anderen Netzen geschützt.

	Schüler-Netz	Lehrer-Netz	Server	Gast-Netz
Mögliche Endgeräte:	Pädagogische Endgeräte (Schul-PCs / Tablets) Schülereigene Endgeräte	Lehrer-Endgeräte (PCs / Tablets) BYOD Endgeräte der Lehrer	Pädagogische Netzressourcen (Server)	Endgeräte von Gästen
WLAN-SSID:	dSchueler	dLehrer	---------	dGaeste
WLAN-Authentifizierung:	WPA-PSK 802.1X	WPA-PSK 802.1X		Sponsor Portal
Zugriff auf:	Internet lokale Ressourcen im Schüler Netz Ressourcen in Server-Netzen	Internet lokale Ressourcen im Lehrer Netz Ressourcen in Server-Netzen	Internet Schüler/Lehrer/Server-Netze	Internet
VLAN:	VLAN 137	VLAN 237	VLAN 337	VLAN 537

Clients aus dem Schüler-Segment können Verbindungen in das eigene/lokale Schüler-Segment, das lokale Server-Segment, alle Remote-Server-Segmente und Verbindungen ins Internet über den Internet-Filter aufbauen. Alle weiteren Verbindungen werden blockiert.

Clients aus dem Lehrer-Segment können Verbindungen in das eigene/ lokale Lehrer-Segment, das lokale Server-Segment, alle Remote-Server-Segmente und Verbindungen ins Internet über den Internet-Filter aufbauen. Alle weiteren Verbindungen werden blockiert.

Clients/Server aus dem Server-Segment können Verbindungen in alle lokalen & remote Server/Schüler/Lehrer-Segmente und ins Internet über den Internet-Filter aufbauen. Alle weiteren Verbindungen werden blockiert.

Clients aus dem Gäste-Segment können Verbindungen **nur** ins Internet über den Internet-Filter aufbauen. Alle weiteren Verbindungen werden blockiert.

6. URL-Filter

Der Zugriff auf das Internet erfolgt transparent, Zugriffe via HTTP und HTTPS werden durch einen URL-Filter geprüft und ggf. blockiert. Die Filterung geschieht nach Kategorien, deren Inhalte laufend aktualisiert werden. Bestimmte Kategorien sind dauerhaft blockiert (siehe unten). Derzeit wird ein User-Interface entwickelt, über das sich die für die Netze einer Schule verantwortlichen Lehrerinnen und Lehrer mittels Kennung und Passwort anmelden können, um weitere Kategorien zu blocken oder freizuschalten.

Zur Abstimmung liegt aktuell folgende Tabelle vor:

Geblockt (dauerhaft)	**Über Web-Interface blockierbar/freischaltbar**
Adult	Alcohol-and-tobacco
Questionable	Dating
Abused-drugs	Swimsuits-and-intimate-apparel
Hacking	Games
Gambling	Military
Weapons	Sex-education
Malware	…
Phishing	
Command-and-control	
Nudity	
Proxy-avoidance-and-anonymizer	
Web-advertisements	

Aufrufe von Domains bzw. URLs der genannten Kategorien werden geblockt. Aufrufe via http führen zu einer entsprechenden Fehlermeldung mit Hinweis auf den URL-Filter. Aufrufe via https können protokollbedingt nur blockiert, aber nicht auf eine Fehlermeldung umgeleitet werden.

7. FAQ

Über welches Medium wird das pädagogische Internet ausgekoppelt?

Der Anschluss erfolgt per Gigabit-Ethernet (Kupfer/RJ45). Speed- und Duplexeinstellungen sind auf auto negotiation konfiguriert.

Kann ich Quality of Service (QoS) nutzen?

Das Verwaltungsnetz, das an den CE-Router angebunden ist, soll von dem Internet-Traffic nicht beeinflusst werden. Daher wird das Verwaltungsnetz priorisiert übertragen. Sämtlicher pädagogischer Internetverkehr wird im Landesnetz-SH in einer entsprechend niedrigeren QoS-Klasse übertragen. Das Setzen eigener durchgehender QoS-Parameter ist nicht möglich.

Ist eine freie Kommunikation von Schulen untereinander in der GBG037 möglich?

Bitte beachten Sie hierzu die Sicherheitspolicy, Textziffer 5.

Können auch andere DNS-Server vergeben werden als die beiden per DHCP vorgegebenen?

Ja, es kann jeder beliebige DNS-Server manuell vergeben werden.

Ist eine direkte Kommunikation zwischen Verwaltungsnetz und pädagogischem Internet über das Landesnetz möglich?

Es ist keine Kommunikation vom Verwaltungsnetz zum pädagogischen Internet möglich/gestattet.

Dauerhaftgeblockte Inhalte in Suchanfragen blockieren – Safesearchenforcement

Bei Suchanfragen über Google, Bing und Yahoo kann der pädagogische Filter die Sicherheitseinstellungen dieser drei genannten Suchmaschinen anpassen.

Hinweis:
Dies funktioniert nur, in nicht verschlüsselten Datenströmen (http)