

Spezifikation für Netzwerkswitche, interne Switche und Netzwerkschnittstellen

Hamburger Energienetze GmbH
Bramfelder Chaussee 130
22177 Hamburg

info@hamburger-energienetze.de
hamburger-energienetze.de



Vorwort

Die Spezifikation wird kontinuierlich und bedarfsgerecht angepasst. Um Veränderungen nachzuvollziehen, enthält diese Spezifikation ein Änderungsverzeichnis, welches Änderungen und Ergänzungen in dem jeweiligen Ausgabestand der Spezifikation aufführt. Bei dem Änderungsverzeichnis wird darauf hingewiesen, dass durch den Auftraggeber nicht garantiert wird, dass alle Änderungen und Ergänzungen enthalten sind.

Änderungen im Dokument

Kapitel	Änderung	Datum
Gesamtes Dokument	- Erstellen des Dokumentes	März 2025
	-	

Inhalt

1. Allgemeines	4
1.1 Geltungsbereich.....	4
1.2 Abweichungen.....	4
1.3 Abwicklung	4
2. Normen und Vorschriften	4
3. Einführung.....	5
4. Allgemeine Anforderungen.....	5
4.1 Virtual Local Area Network (VLAN).....	5
4.2 Redundanzprotokolle.....	5
4.3 Diagnosefunktion	5
4.4 Simple Network Management Protocol (SNMP)	6
4.5 Portspiegelung.....	6
4.6 Portstatistiken und Portinformationen	6
4.7 Small Form-factor Pluggable (SFP)-Informationen	7
5. Diskret ausgeführte Switche.....	7
5.1 Mechanische und konstruktive Anforderungen	7
5.2 Hilfsspannungsversorgung.....	7
5.3 Life- und Relaiskontakte	8
5.4 Ausführung und Anzahl an Interfaces.....	8
5.5 Managementfunktionen und Konfiguration	9
5.6 Link Layer Discovery Protocol (LLDP)	10
5.7 Sicherheit	10
5.8 Uhrzeitsynchronisierung bzw. Uhrzeitmanagement	10

1. Allgemeines

1.1 Geltungsbereich

Diese Spezifikation gilt für Netzwerkschalter im Stations-LAN, sowohl für diskret ausgeführte als auch für interne Switches in Geräten der Schutz- und Leittechnik.

1.2 Abweichungen

Abweichungen von dieser Spezifikation sind im Angebot detailliert zu beschreiben. Abweichungen bei der Lieferung sind nur zulässig, wenn eine schriftliche Zustimmung seitens des Auftraggebers vorliegt.

Die Zustimmung zu Abweichungen hat der jeweilige technische Bearbeiter des Auftraggebers bei dem zuständigen Bearbeiter der Spezifikation einzuholen.

1.3 Abwicklung

Die Abwicklung und der Schriftverkehr müssen in deutscher Sprache erfolgen. Dieses gilt auch für die gesamte technische Dokumentation.

Zu jedem Zeitpunkt im Projekt muss eine technisch-verantwortliche Person (Auftragnehmer) für den Auftraggeber zur Verfügung stehen. Ein Wechsel der Verantwortlichkeit seitens des Auftragnehmers muss dem Auftraggeber schriftlich angezeigt werden.

2. Normen und Vorschriften

Die Beachtung der vorliegenden Spezifikation ist zwingend. Die vorliegende Spezifikation entbindet den Auftragnehmer nicht von seiner Pflicht, die Errichtung, Ertüchtigung und Erweiterung entsprechend denen in der Bundesrepublik Deutschland

- aktuellen geltenden einschlägigen Normen (DIN, DIN-VDE) oder
- vergleichbaren geltenden Europäischen Normen (EN) oder
- vergleichbaren internationalen Normen (IEC und IEEE) sowie
- geltenden anerkannten Regeln der Technik

auszuführen.

Eventuelle Abweichungen zwischen den einschlägigen Normen/ Vorschriften und der Spezifikation sind dem Auftraggeber unverzüglich schriftlich anzuzeigen, der Auftraggeber wird erforderlichenfalls über die Ausführung entscheiden.

Bei Nichtbeachtung gehen notwendige Änderungen zu Lasten des Auftragnehmers.

3. Einführung

Die nachfolgend aufgeführten Anforderungen gelten für Netzwerkschwitche im Stations- LAN.

4. Allgemeine Anforderungen

Die nachfolgend aufgeführten Punkte gelten sowohl für diskret ausgeführte Switches, wie auch für Switches, welche in Geräten der Schutz- und Leittechnik (z.B. BPCUs und PIUs) integriert sind.

4.1 Virtual Local Area Network (VLAN)

Die Netzwerkschwitches müssen VLANs nach IEEE 802.1Q unterstützen. Es müssen mindestens bis zu 64 VLANs gleichzeitig verarbeitet werden können.

Zusätzlich müssen folgende Funktionen unterstützt werden:

- Protokollbasiertes VLAN
- VLAN Unaware Mode
- MAC-Adressen basiertes VLAN

4.2 Redundanzprotokolle

Es müssen mindestens nachstehende Redundanzprotokolle unterstützt werden.

4.2.1 (Rapid) Spanning Tree Protocol (RSTP)

Es muss das Rapid Spanning Tree Protocol (RSTP) nach IEEE 802.1D-2004 unterstützt werden.

RSTP muss auf allen Interfaces unterstützt werden.

Es müssen bis zu 40 RSTP-Switches in einer Ringtopologie unterstützt werden.

Zu älteren Switches, welche mit dem Spanning Tree Protocol (STP) nach IEEE 802.1d kommunizieren, muss das Gerät abwärtskompatibel sein.

Die für RSTP notwendigen Parameter müssen durch den Anwender frei konfigurierbar sein:

- Hello-Time [1 s bis 2 s]
- Forward-Delay
- Bridge-Priority [0 bis 61440 in 4096er-Schritten]
- Max-Age
- Tx-Holds
- Pfadkosten je Interface [0 bis 2.000.000]
- Port-Priority je Interface

RSTP muss global und je Interface aktivierbar bzw. deaktivierbar sein.

Interfaces für einzelne Endgeräte ohne redundante Anbindung müssen als Edge-Port konfigurierbar sein. Dieses muss manuell bzw. automatisch je Interface möglich sein.

4.3 Diagnosefunktion

4.3.1 Syslog

Das Gerät muss zur Protokollierung Syslog unterstützen. Es muss ein lokales Systemlogging auf dem Gerät, wie auch ein Remote-Syslog möglich sein.

Der Schweregrad einer zu protokollierenden Syslog-Meldung muss für beide Fälle konfigurierbar sein.

Sofern seitens der Syslog-Implementierung alle Informationen unter einer Facility abgelegt werden, ist diese bei Verwendung von Remote-Syslog mit dem AG abzustimmen.

Für ein Remote-Syslog müssen mindestens zwei Syslog-Server hinterlegt werden können.

4.4 Simple Network Management Protocol (SNMP)

Es muss SNMP v3 unterstützt werden.

Bei SNMPv3 muss Authentifizierung und Übertragungsverschlüsselung (authPriv) unterstützt werden. Es müssen HMACMD5 und HMACSHA als Authentifizierungsprotokolle unterstützt werden. Für die Übertragungsverschlüsselung müssen Data Encryption Standard (DES) und Advanced Encryption Standard (AES) mit einer Schlüssellänge von 128 Bit (AES-128) unterstützt werden.

Die Benutzer, welche über SNMP Zugang zum Gerät haben, müssen frei konfiguriert werden können. Ein festes Mapping der Benutzer Administrator und User auf bestimmte Community-Namen bei SNMPv1/2 für den Lese- und Schreibzugang ist nicht zugelassen. Ebenfalls müssen die für einen SNMP-Zugang zugelassenen IP-Adressen hinterlegt werden können.

Sofern die MAC-Adressen nicht als interfacespezifische Neighbourhood-Informationen in die LLDP-Tabelle übernommen werden, muss der Switch die SNMP-Abfrage der Forwarding-Database (FDB) ermöglichen.

Neben der Abfrage per SNMP sind durch ein Ereignis getriggerte Nachrichten (SNMP-Taps) zu unterstützen.

Es müssen mindestens zwei Manager als Trap-Log-Server hinterlegt werden können. Jedem Trap-Log-Server ist eine IPv4-Adresse und ein Name zuzuordnen.

Bei nachstehenden Bedingungen müssen min. SNMP-Taps gesendet werden können:

- Neustart des Gerätes
- Link-Up/Down an einem Interface
- Neue RSTP-Root
- Topologieänderung
- Zustandsänderung des Life- bzw. Relaiskontaktes
- Grenzwertüberschreitung einer je Interface spezifischen Netzlast
- Grenzwertüberschreitung einer je PoE-Interface spezifischen Ausgangsleistung
- Lernen neuer MAC-Adressen an einem Interface
- Login-Authentifizierung

4.5 Portspiegelung

Diskret ausgeführte Switches müssen folgende Möglichkeiten zur Portspiegelung unterstützen:

- 1:1 = 1 Quell-Interface auf 1 Ziel-Interface
- N:1 = N-Quell-Interfaces auf 1 Ziel-Interface
- VLAN:1 = Ein VLAN (unabhängig vom Quell- oder Zielinterface) auf 1 Ziel-Interface

Die Portspiegelung muss global ein- bzw. ausgeschaltet werden können.

4.6 Portstatistiken und Portinformationen

Je verfügbaren Interface ist innerhalb des Switches eine Statistik bzw. eine Informationstabelle zu führen, welche min. folgende Angaben beinhaltet:

- Nr. des Interfaces
- Name
- Link-Zustand (up/down)

- Ausgewählte Geschwindigkeit bei Autonegotiation
- Ausgewählte Duplex-Betriebsart bei Autonegotiation
- Eingestellte Geschwindigkeit bei fixer Betriebsart
- Eingestellte Duplex-Betriebsart bei fixer Betriebsart
- Statistiken über empfangene und gesendete Frames je Interface
Die Statistiken müssen insbesondere die Anzahl an Frames mit CRC-Fehlern und Fragmenten beinhalten. Ebenfalls müssen die Anzahl an Frames, bei denen eine Collision bzw. Late-Collision erkannt wurde, protokolliert werden.
- Netzlast je Interface
- Empfangene RSTP-Parameter je Interface
- RSTP-Port-Rolle je Interface
- RSTP-Port-Zustand je Interface

Die Portstatistiken und Portinformationen müssen von einem SNMP-Manager abgefragt werden können.

4.7 Small Form-factor Pluggable (SFP)-Informationen

Für alle im Gerät installierten SFP-Transceiver muss eine Tabelle mit deren Eigenschaften geführt werden:

- Interface-Nr., in dem der SFP installiert ist
- SFP-Typenbezeichnung
- Seriennummer des SFP

5. Diskret ausgeführte Switche

Nachstehend aufgeführte Punkte gelten ausschließlich für diskret ausgeführte Switche im Stations -LAN.

5.1 Mechanische und konstruktive Anforderungen

Alle Switche müssen für den Einsatz in Umspannwerken und Schaltanlagen der elektrischen Energieverteilung geeignet sein. Insbesondere müssen die Geräte die Anforderungen der IEC 61850-3 und der IEEE 1613 erfüllen. Entsprechende Eignungsnachweise sind durch den AN nachzuweisen.

Je nach Anwendungsfall sind die Netzwerkschwitche zur

- 19-Zoll Rack-Montage
- DIN-Hutschienenmontage

auszuführen.

Bei der 19-Zoll-Ausführung darf der Netzwerkschwitch max. eine Höhen-Teilungseinheit (HE) beanspruchen. Die maximale Tiefe bei dieser Ausführung beträgt ohne montierte Stecker und Kabel 400 mm.

Der Netzwerkschwitch muss über seine gesamte Betriebs- und Lebenszeit wartungsfrei sein. Er darf keine Batterien haben, muss lüfterlos und frei von sonstigen rotierenden Teilen sein.

Die Anschlüsse der jeweiligen Netzwerkkinterfaces müssen auf der Gerätefront (Draufsicht bei montiertem Netzwerkschwitch) sein. Gleiches gilt für die Anordnung von LEDs.

Der Netzwerkschwitch muss mindestens der Schutzart IP30 entsprechen.

5.2 Hilfsspannungsversorgung

Das Gerät muss über ein Weitbereichsnetzteil mit 110 V bis 230 V AC/DC verfügen.

Das Netzteil ist singulär auszuführen. Ein redundantes Netzteil muss als Bestelloption verfügbar sein und ggf. nachgerüstet werden können.

Der Anschluss der Hilfsspannungsversorgung hat über einen abnehmbaren Klemmenblock zu erfolgen, sodass ein Gerätewechsel ohne Abklemmen der Hilfsspannungsversorgung möglich ist. Der Klemmenblock muss durch eine Verschraubung am Gerät gesichert werden. Der Klemmenblock muss den Anschluss von Leitern mit einem Querschnitt von bis zu 1,5 mm² ermöglichen.

Nach Ausfall der Hilfsspannungsversorgung muss ein automatischer Wiederanlauf ohne Parametersatzverlust erfolgen.

5.3 Life- und Relaiskontakte

Der Netzwerkschalt muss über mindestens einen Relaiskontakt verfügen, welcher als Life-Kontakt des Gerätes genutzt werden kann.

Der Relaiskontakt ist als Wechsler auszuführen, mindestens jedoch als Öffner. Ein reiner Lifekontakt als Schließer ist nicht zugelassen.

Der Relaiskontakt ist potentialfrei auszuführen. Es müssen Spannungen bis zu 230 V AC und 250 V DC geschaltet werden können.

Der Anschluss der Life- und Relaiskontakte hat über einen abnehmbaren Klemmenblock zu erfolgen, sodass ein Gerätewechsel ohne Abklemmen der Life- und Relaiskontakte möglich ist. Der Klemmenblock muss durch eine Verschraubung am Gerät gesichert werden. Der Klemmenblock muss den Anschluss von Leitern mit einem Querschnitt von bis zu 1,5 mm² ermöglichen.

Im spannungslosen Zustand ist der Lifekontakt geschlossen, nach dem Hochlaufen des Gerätes bzw. im Normalbetrieb öffnet der Lifekontakt. Ein Geräteausfall muss dazu führen, dass der Lifekontakt abfällt. Ein abgefallener Lifekontakt ist über eine Störungs-LED anzuzeigen.

Weitere ausgewählte Betriebszustände müssen per Parametrierung auf den Life- bzw. Relaiskontakt rangiert werden können.

5.4 Ausführung und Anzahl an Interfaces

5.4.1 Netzwerkschalt

Netzwerkschalt in der 19"-Ausführung, welche im Stations-LAN eingesetzt werden, müssen mindestens über 24 Interfaces verfügen.

Alle Interfaces müssen Übertragungsraten von 10/100/1000 Mbit/s unterstützen, welche je nach Anwendungsfall als optische oder elektrische Interfaces auszuführen sind. Elektrische Interfaces müssen Autonegotiation (Duplex: Auto/HDX/FDX) und Autocrossing ermöglichen.

Beide Funktionen müssen auch per Parametrierung deaktivierbar und auf einen festen Parameter konfigurierbar sein.

Die nicht PoE-fähigen-Interfaces müssen den Einsatz von SFP gemäß Abschnitt 5.4.3 ermöglichen.

Je nach Anwendungsfall muss mindestens ein Interface je Switch PoE-fähig sein. Die PoE-Klasse und das Leistungsbudget der PoE-Interfaces muss an die Anwendungsfälle angepasst sein und ist vom AN passend zu wählen.

Wenn eine gewisse Anzahl an Interfaces über Medienmodule bereitgestellt wird, müssen die Module im laufenden Betrieb und ohne eine Abschaltung des Schalters getauscht werden können (hot pluggable).

5.4.2 Kompaktschalt zur DIN-Hutschienenmontage

Netzwerkschalt zur DIN-Hutschienenmontage, welche im Stations-LAN eingesetzt werden, müssen mindestens über acht Interfaces verfügen.

Alle Interfaces müssen Übertragungsraten von 10/100/1000 Mbit/s unterstützen, welche je nach Anwendungsfall als optische oder elektrische Interfaces auszuführen sind. Elektrische Interfaces müssen Autonegotiation (Duplex: Auto/HDX/FDX) und Autocrossing ermöglichen. Beide Funktionen müssen auch per Parametrierung deaktivierbar und auf einen Fest Parameter konfigurierbar sein.

Je nach Anwendungsfall muss mindestens ein Interface je Switch PoE-fähig sein. Die PoE-Klasse und das Leistungsbudget der PoE-Interfaces muss an die Anwendungsfälle angepasst sein und ist von AN passend zu wählen.

Netzwerkschalt zur DIN-Hutschienenmontage, welche ausschließlich zur Sensoranbindung über Modbus TCP eingesetzt werden, müssen über mindestens 16 Interfaces verfügen.

Alle Interfaces müssen als Fast-Ethernet 100-Base-Tx Interface ausgeführt sein und PoE-fähig sein. Die PoE Klasse und das Leistungsbudget der PoE-Interfaces muss an die Anwendungsfälle angepasst sein und ist von AN passend zu wählen.

5.4.3 Small Form-factor Pluggable (SFP)

Die Festlegungen für SFP gelten für alle Schalttypen.

Es müssen mindestens folgende Typen an SFP unterstützt werden:

- 10/100/1000-Base-T
 - Übertragungsrate: 10/100/1000 Mbit/s
 - Anschluss: RJ-45
 - Kategorie: >CAT5
 - Autonegotiation (Duplex: Auto/HDX/FDX)
 - Autocrossing (Automatische Konfiguration von MDI – MDI(X))
- 100Base-FX
 - Übertragungsrate: 100 Mbit/s
 - MM (Multi-Mode)
 - Anschluss: LC
 - Kategorie: 50/125 oder 62.5/125 µm
- 1000Base-SX
 - Übertragungsrate: 1000 Mbit/s
 - MM (Multi-Mode)
 - Anschluss: LC
 - Kategorie: 50/125 oder 62.5/125 µm

SFP müssen im laufenden Betrieb und ohne eine Abschaltung des Switches getauscht werden können (hot pluggable). Das Entfernen eines SFP darf nicht zum Verlust der Interface-Konfiguration führen. Ein Interface ohne SFP muss per Konfiguration auch deaktivierbar sein.

5.5 Managementfunktionen und Konfiguration

Zur Parametrierung und Konfiguration, sowie zur Diagnose und Wartung müssen mindestens folgende Protokolle bzw. Dienste unterstützt werden:

- HTTPS
- HTTP
- SSHv2
- Telnet
- CLI über eine V.24-Schnittstelle

Die Protokolle bzw. Dienste müssen einzeln deaktivierbar sein.

Die Konfiguration des Netzwerkschwitches muss über einen Web-Server per HTTPS bzw. HTTP möglich sein. Sämtliche Parameter müssen über diese Art des Managementzugriffes auslesbar und konfigurierbar sein. Ebenfalls muss ein Firmwareupdate sowie das Sichern und Laden von Parametersätzen über den Web-Server möglich sein.

Lediglich zur Erstkonfiguration (neues Gerät ab Werk, oder nach einem Reset auf Werkseinstellungen) eines Netzwerkschwitches ist ein ausschließlicher Managementzugriff über ein CLI zulässig. Der Web-Server muss ohne die zusätzliche Installation einer Java-Laufzeitumgebung und in jedem Standard-Webbrowser auf dem Servicerechner des Auftraggebers möglich sein. Der netzwerkbasierte Managementzugriff muss einem VLAN (Management-VLAN) zugeordnet werden können.

Zur Parametersatzsicherung muss es möglich sein, dass die Konfiguration nach einer Änderung und Sicherung auf dem Gerät, automatisch auf ein Filesystem übertagen und archiviert wird. Hierzu muss der Netzwerkschwitch folgende Protokolle unterstützen:

- TFTP
- SFTP

5.6 Link Layer Discovery Protocol (LLDP)

Es muss das Link Layer Discovery Protocol nach IEEE 802.1AB unterstützt werden.

LLDP muss global und pro Interface ein- bzw. ausschaltbar sein.

Ebenfalls muss das Sendeintervall für LLDP-Frames einstellbar sein.

Die LLDP-Betriebsart muss pro Interface festgelegt werden können:

- es dürfen nur LLDP-Frames empfangen werden
- es dürfen nur LLDP-Frames gesendet werden
- es dürfen LLDP-Frames empfangen und gesendet werden.

Die LLDP-Neighbourhood-Informationen sind je Interface in einer Tabelle zu führen und müssen von einem SNMP-Manager abgefragt werden können.

An Interfaces an denen nicht LLDP-fähige Endgeräte angeschlossen sind, sind die MAC-Adressen aus der Forwarding-Database (FDB) als interfacespezifische Neighbourhood-Informationen in die LLDP-Tabelle zu übernehmen. Auch diese Informationen müssen von einem SNMP-Manager (NMS) abgefragt werden können.

5.7 Sicherheit

5.7.1 Benutzerverwaltung

Sämtlicher Zugang auf den Netzwerkschwitch muss über eine rollenbasierte Benutzerverwaltung (RBAC) geschützt sein.

Die Benutzerverwaltung (Rolle, Benutzer und Passwort) muss lokal auf dem Gerät angelegt und verwaltet werden können. Benutzernamen und Passwörter müssen frei konfigurierbar sein. Jedem Benutzer muss eine Rolle mit zugewiesenen Rechten zugeordnet werden können. Es ist mindestens in die Rolle Administrator (Vollzugriff) und User (Lesezugriff) zu unterscheiden. Es muss möglich sein, ausgewählte Benutzer zu sperren, ohne dessen Profil vom Gerät zu löschen.

Jede Authentifizierung, auch eine erfolglose, ist zu protokollieren.

Alternativ muss die Benutzerverwaltung und die Authentifizierung auch global (z.B. über Active Directory) verwaltet bzw. ausgeführt werden können. Hierzu muss der Netzwerkschwitch eine Authentifizierung über Remote Authentication Dial-In User Service (RADIUS) und Lightweight Directory Access Protocol (LDAP) ermöglichen.

5.7.2 Port-Sicherheit

Es müssen mindestens folgende Verfahren zur Port-Sicherheit unterstützt werden:

- MAC-basierte Port-Sicherheit,
- Port-basierte Zugangskontrolle mittels 802.1X-Authentifizierung
- MAC-Authentifizierungs-Bypass (MAB)

5.8 Uhrzeitsynchronisierung bzw. Uhrzeitmanagement

Die Management-Umgebung des Switches muss in der Uhrzeit synchronisiert sein, damit für eine Protokollierung (z.B. Gerätelogfiles oder Syslog) die Ereignisse zeitlich korrekt eingeordnet werden.

Zum Uhrzeitmanagement müssen die für den Einbauort gültige Zeitzone sowie die gültigen Regeln zur Sommer- und Winterzeitumstellung hinterlegt werden können.

5.8.1 Network Time Protocol (NTP)

Der Netzwerkschwitch muss sowohl als NTP-Client sowie als NTP-Server konfigurierbar sein.

Es muss NTP gemäß „RFC 5905 – NTPv4 Protokoll und Algorithmus“ unterstützt werden, mindestens jedoch SNTP gemäß „RFC 4330 – Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI“.

Die Synchronisierung hat im Unicast-Mode zu erfolgen. Das Anfrageintervall muss konfigurierbar sein.

Es müssen per Konfiguration mindestens zwei Zeitserver angegeben werden können.
Die Zeitquelle muss auf einen Ausfall hin überwacht werden (Ausbleiben der Synchronisier Nachrichten).
Die Telegramme zur Uhrzeitsynchronisierung müssen einem VLAN zugeordnet werden können.