Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Strassen ASTRA

RICHTLINIE

IP-NETZ BSA

Ausgabe 2017 V1.30
ASTRA 13040

Impressum

Autor(en) / Arbeitsgruppe V1.30

Jean-Paul Schnetz	(ASTRA DS, Vorsitz)
Jolanda Geringer	(ASTRA DS)
Martin Wyss	(ASTRA I-B, FG BSA)
Markus Eisenlohr	(ASTRA I-FU, FG BSA)
Markus Berger	(ASTRA I-FU, FG BSA)
Daniel Gähwiler	(CSI Consulting AG)
Patrick Gerber	(CSI Consulting AG)

Autor(en) / Arbeitsgruppe bis V1.20

Markus Glanzmann	(ASTRA N-ST)
Urs Luther	(ASTRA N-ST)
Eugen Fuchs	(ASTRA N-ST)
Bendicht Hirschi	(ASTRA I-FU, FG BSA)
Jörg Dreier	(ASTRA N-VMZ)
Markus Riederer	(ASTRA N-VIM)
Robert Hämmerli	(ASTRA I-F4)
Andreas Wüst	(GE VII)
Grégory Champion	(GE IX)
Ivo Achermann	(GE X)
Manfred Lussmann	(GE XI)
Brundo Widrig	(GE XI)
Ywan Wyser	(ASTRA N-VMZ)

Übersetzung

Sprachdienste ASTRA	(Originalversion in Deutsch)

Herausgeber
Bundesamt für Strassen ASTRA
Abteilung Strassennetze N
Standards und Sicherheit der Infrastruktur SSI
3003 Bern

Bezugsquelle
Das Dokument kann kostenlos von www.astra.admin.ch heruntergeladen werden.

Vorwort

Die Betriebs- und Sicherheitsausrüstungen (BSA) tragen einen erheblichen Teil zur Sicherheit der Tunnel und offenen Strecken des schweizerischen Nationalstrassennetzes bei.

Damit diese Anlagen effizient genutzt und betrieben werden können, muss eine homogene, leistungsfähige und hochverfügbare Kommunikationsinfrastruktur zur Verfügung stehen.

Die vorliegende Richtlinie beschreibt eine schweizweit einheitliche und durchgängige BSA-Kommunikationsinfrastruktur.

Die BSA-Kommunikationsinfrastruktur bildet eine tragfähige und einheitliche Basis, welche es dem ASTRA ermöglicht, die BSA weiter auszubauen, aber auch neue Lösungen im Bereich Verkehrsmanagement oder Vernetzung der Fahrzeuge mit der Infrastruktur zu realisieren.

Bundesamt für Strassen

Jürg Röthlisberger
Direktor

Inhaltsverzeichnis

1 Einleitung

1.1 Zweck des Dokumentes

Diese Richtlinie hat zum Ziel, den Aufbau der Kommunikationsinfrastruktur für die Betriebs- und Sicherheitsausrüstungen (BSA) der Nationalstrassen zu standardisieren und auf ein modernes in die Zukunft gerichtetes Fundament zu stellen.

Das Dokument beschreibt die angestrebte Netzarchitektur für den Backbone und die lokalen Kommunikationsinfrastrukturen in den Gebietseinheiten (GE) mit den Schnittstellen zu den BSA RZ, zur VMZ-CH, zu anderen GE, zu den Basisdiensten IP-Netz BSA, zu den Kantons- und Bundesnetzen, zu den Partnernetzen wie der Swisscom und zu übrigen Fremdnetzen wie dem Internet.

Neben der Netzarchitektur werden die Anforderungen an die einzusetzenden Netzwerkgeräte und Services im IP-Netz BSA beschrieben.

Zusätzlich werden die Standardisierung der IP-Adressierung, die Verwendung von Support Systeme für das IP-Adressmanagement, die Konfiguration von DNS- und DHCP-Services, die Netzwerk-Security und die Anforderungen an das Network Management für den Aufbau und Betrieb des IP-Netzes BSA über diese Richtlinie vorgegeben.

Im abschliessenden Kapitel werden die betrieblichen Vorgaben und Anforderungen aufgeführt.

1.2 Geltungsbereich

Die Richtlinie gilt grundsätzlich für alle BSA-Kommunikationsnetzwerke, insbesondere für folgende Fälle:

- Ersatz resp. Erneuerung eines gesamten BSA-Kommunikationsnetzwerkes einer GE bei End of Life;
- Teilerneuerung (bspw. Migration auf IPv6, Ablösung NMS) eines gesamten BSA-Kommunikationsnetzwerkes einer GE;
- Erweiterungen oder Erneuerung eines Teils des BSA-Kommunikationsnetzwerkes einer GE (bspw. Abschnitt), sofern eine Vorinvestition sinnvoll und wirtschaftlich vertretbar ist.

Das IP-Netz BSA ersetzt sämtliche bisher existierende lokalen Kommunikationsnetze in den Gebietseinheiten im Bereich der BSA.

1.3 Adressaten

Die Richtlinie wendet sich an:

- Fachspezialisten des ASTRA;
- Fachspezialisten der Gebietseinheiten;
- Ingenieurbüros und Unternehmungen, die im Auftrag des ASTRA Tätigkeiten an den Kommunikationsinfrastrukturen BSA ausführen.

1.4 Inkrafttreten und Änderungen

Die vorliegende Richtlinie tritt am 07.12.2017 in Kraft. Die „Auflistung der Änderungen “ ist auf Seite 44 dokumentiert.

2 Referenzarchitektur

2.1 Definitionen

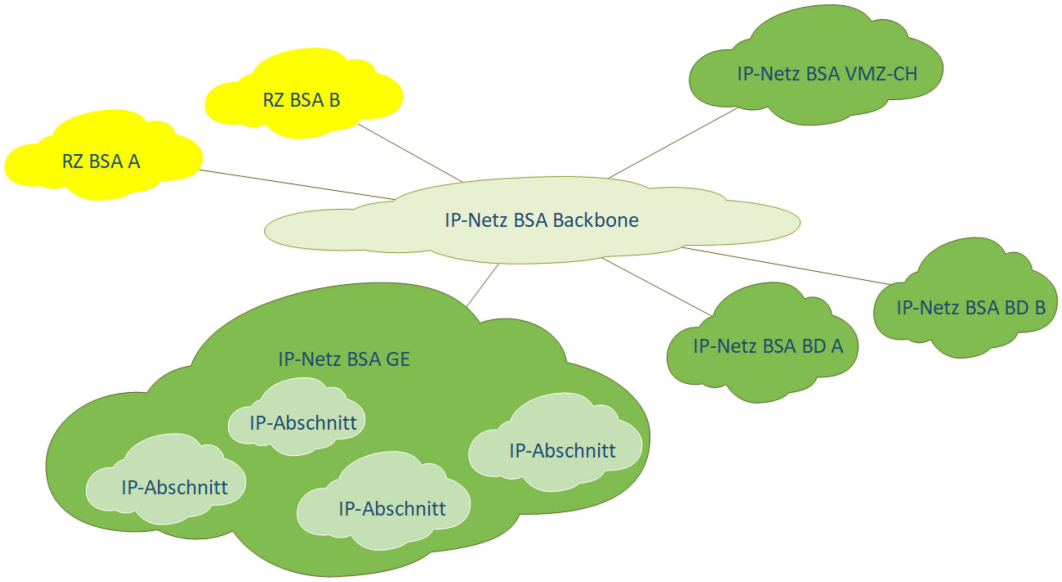

Abb. 2.1 Begriffe IP-Netz BSA

Die BSA-Kommunikationsinfrastruktur einer GE bezeichnet man als «IP-Netz BSA GE».

Als «IP-Abschnitt» bezeichnet man ein lokales Teilnetz des IP-Netz BSA GE, das in sich autonom funktionsfähig ist. D.h. in einem IP-Abschnitt ist die lokale Kommunikation zwischen den Anlagen des Netzabschnittes sichergestellt.

Das Kommunikationsnetz «IP-Netz BSA VMZ-CH» der VMZ-CH wird analog eines IP-Netzes BSA GE behandelt.

Das Kommunikationsnetz «IP-Netz BSA BD A/B» wird analog eines IP-Netzes BSA GE behandelt, besteht aber nur aus einem Backbone-Anschluss und einer standortbezogenen Netzwerkinfrastruktur.

Als «IP-Netz BSA Backbone» wird die Kommunikationsinfrastruktur bezeichnet, die die IP-Netze BSA GE, die IP-Netz BSA VMZ-CH, die IP-Netze BSA BD A/B und die RZ BSA A/B untereinander verbindet.

Die Gesamtheit der IP-Netze BSA GE, der IP-Netze BSA BD A/B, des IP-Netzes BSA VMZ-CH und des IP-Netzes BSA Backbone wird als «IP-Netz BSA» bezeichnet.

Der Access-Layer in den RZ BSA, das BSA RZ LAN, ist nicht Teil des IP-Netzes BSA.

2.2 Abgrenzung

Das IP-Netz BSA ist als SCADA[1]-Kommunikationsnetz ausgelegt und nutzt das IP-Netz BSA Backbone. Das IP-Netz BSA Backbone ergänzt das bestehende Kommunikationsangebot der Bundesverwaltung («BV-Netz») mit einer SCADA-tauglichen Vernetzung und ist vollständig getrennt vom heutigen Netz der Bundesverwaltung aufgebaut, auch wenn teilweise die gleichen ASTRA Standorte erschlossen werden.

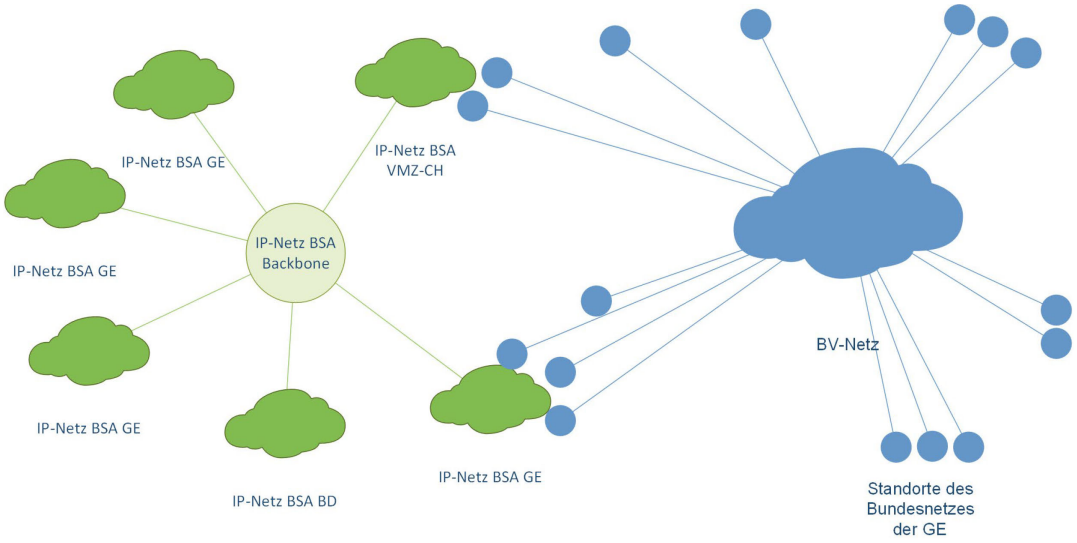

Abb. 2.2 Strikte Trennung IP-Netz BSA (grün) vom BV-Netz (blau)

Das vorliegende Dokument behandelt ausschliesslich die Gesamtlösung IP-Netz BSA.

2.3 Abgrenzung LWL

Diese Richtlinie beschreibt nicht die Ausgestaltung des LWL-Netzes des ASTRA, geht aber für die Ausgestaltung der Netzarchitektur von folgenden Annahmen im Bereich LWL aus:

- Es sind entlang den Nationalstrassen genügend freie LWL bzw. Fasern zur Nutzung durch das IP-Netz BSA vorhanden;
- Ebenso sind die notwendigen ASTRA Standorte wie Werkhöfe, Leitzentralen durch genügend freie LWL von den Nationalstrassen her erschlossen;
- Die LWL-Infrastruktur des ASTRA erfüllt gewisse qualitative Mindestanforderungen bspw. im Bereich Material und Bau, sodass für die Netzwerkarchitektur IP-Netz BSA keine Einschränkungen vorgegeben werden müssen.

Die weiteren Details zu den LWL-Kabelanlagen des ASTRA sind der Richtlinie 13022 [6] zu entnehmen.

[1] SCADA-Systeme (Supervisory Control and Data Acquisition) oder auch ICS- bzw. DCS-Systeme (Industrial Control Systems bzw. Distributed Control Systems) sind vernetzte Computer-Systeme (Leitsysteme) für die Überwachung, Steuerung und Optimierung von Industrie-Anlagen.

2.4 Grundsätze und Übersicht

Eine hohe Verfügbarkeit und ein zuverlässiger Schutz (Security) sind zentrale Anforderungen für die Definition der Netzarchitektur IP-Netz BSA. Daraus für die Architektur abgeleitet gelten folgende Grundregeln:

- Das Design ist auf Ebene Gerät und LWL-Verbindungen durchgängig redundant und weist keine Komponenten auf, die einen Single Point of Failure darstellen:
  - Ein Einzelausfall (bspw. ein defektes Netzwerkelement oder ein LWL-Unterbruch) darf nicht zu einem Ausfall des gesamten IP-Netzes BSA GE führen;
  - Ein Einzelausfall darf nicht zu einem Ausfall eines IP-Abschnitts innerhalb des IP-Netzes BSA GE führen;
  - Ein Einzelausfall führt im Netzwerk höchstens zu einem Redundanzverlust;
  - Ein Einzelausfall darf nicht zu einem Ausfall von redundant angeschlossenen Anwendungen/Geräte im Accessbereich führen.
- Ein Einzelausfall eines Access-Switches darf zu einem Ausfall von Anwendungen/Geräte führen, die nicht redundant an diesem Access-Switch angeschlossen sind bspw. Kameras;
- Ein unabhängiger Doppelausfall darf zu einem Service-Ausfall führen.
- Das Netzwerk selbst muss bereits aufgrund der Struktur und Netzwerktopologie einen hohen Grad an Ausfallsicherheit ausweisen. Dabei ist vor allem die LWL-Topologie zu berücksichtigen und allenfalls anzupassen, damit Redundanzen geschaffen bzw., genutzt werden können.

Das Kommunikationsnetzwerk IP-Netz BSA hat eine schweizweite Flächendeckung und erschliesst alle ASTRA Infrastruktur-Standorte, Leitzentralen und Rechenzentren. Es ist wie folgt strukturiert:

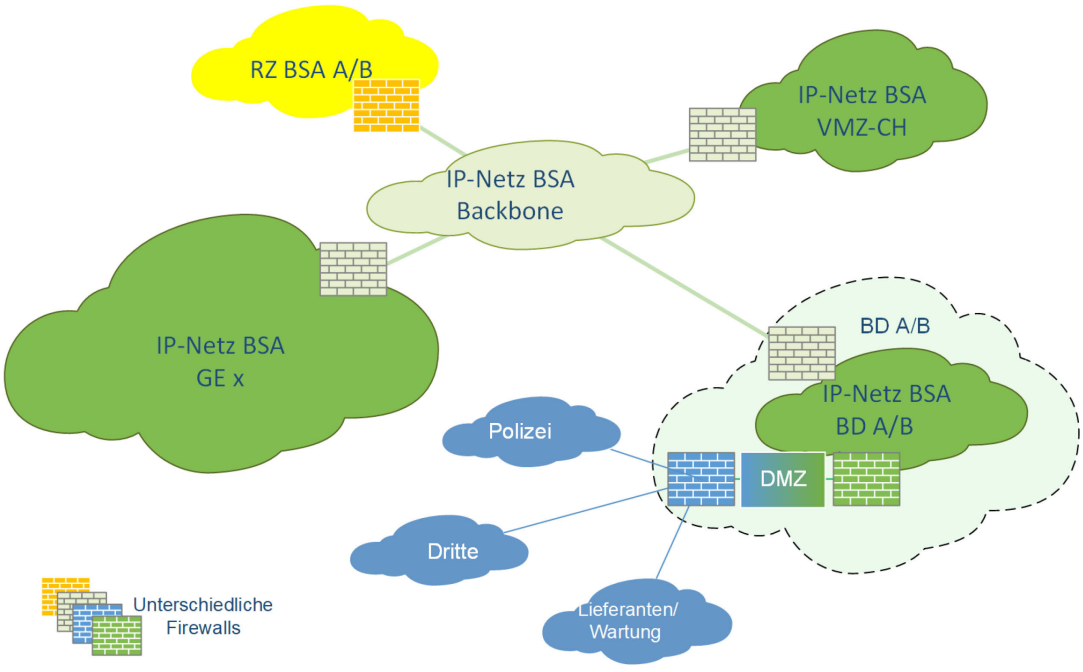

Abb. 2.3 Struktur IP-Netz BSA

Die **IP-Netze BSA GE** sind eigenständige Netzwerke, welche die BSA der Nationalstrassen begrenzt auf den Verantwortungsbereich der jeweiligen Gebietseinheit erschliessen.

Das IP-Netz BSA GE ist in verschiedene **IP-Abschnitte** aufgeteilt. Diese IP-Abschnitte stellen die lokale Kommunikation zwischen den Anlagen des IP-Abschnittes sicher und sind in sich weitgehend autonom funktionsfähig.

Die IP-Abschnitte werden von den **Erschliessungsringen** der jeweiligen GE untereinander verbunden und bilden so jeweils ein IP-Netz BSA GE.

Das **IP-Netz BSA Backbone** stellt die Verbindung von den IP-Netzen BSA GE zur VMZ-CH, zu den RZ BSA und zu den IP-Netzen BSA anderer GE sicher.

Damit die Gebietseinheit den sicheren Betrieb der Anlagen garantieren kann, wird jedes IP-Netz BSA GE mit einer Firewall vom IP-Netz BSA Backbone getrennt.

Alle anderen Netzübergänge von den IP-Netzen BSA GE zu bestehenden Partnern (Polizei, Lieferanten, Services von Dienstleistern) müssen grundsätzlich über die DMZ der Basisdienste im **IP-Netz BSA BD** geführt werden.[2]

Über das IP-Netz BSA Backbone sind ausgewählte Netzressourcen des Bundes erreichbar und nutzbar. Das IP-Netz BSA Backbone ist ebenfalls über Firewalls/Transitzonen von den übrigen Netzen des Bundes zu trennen.

Innerhalb der RZ BSA A/B sind die Netzwerkzonen für die BSA-Fachapplikationen ebenfalls über Firewalls/Transitzonen von den übrigen Zonen der RZ zu trennen.

2.5 Erschliessungsringe IP-Netz BSA GE

Das IP-Netz BSA GE besteht aus den Erschliessungsringen und den zugehörigen Access-Bereichen, den sogenannten IP-Abschnitten, an dem die IP-fähigen Geräte der BSA angeschlossenen werden. Die Erschliessungsringe bilden den Core-Layer eines IP-Netzes BSA GE. Die IP-Abschnitte bilden den Access-Layer, auf einen zusätzlichen Aggregation- oder Distribution-Layer wird verzichtet.

Eine Verbindung über einen Abschnitt hinaus erfolgt ausschliesslich über die Erschliessungsringe.

Die Erschliessungsringe und die Access-Bereiche sind mit getrennten aktiven Komponenten realisiert. Während die aktiven Komponenten eines Access-Bereichs einem einzelnen IP-Abschnitt zugeordnet sind und den Netzwerkanschluss für Enggeräte bereitstellen, führen die aktiven Komponenten der Erschliessungsringe die Ketten von Access-Switches zusammen und stellen die übergeordnete Kommunikation sicher. An den Komponenten der Erschliessungsringe dürfen keine Endgeräte angeschlossen werden.

An Routern terminieren beide Seiten der Ketten. Geografisch müssen deren Standorte nicht unbedingt am Anfang und Ende eines IP-Abschnitts stehen, sondern nur getrennt sein (z.B. Haupt und Nebenzentrale, getrennte Räume bzw. unterschiedliche Brandabschnitte oder Verlegen des einen Routers in den nächsten Netzabschnitt). Jeder Router ist mit mindestens zwei anderen über getrennte Faserwege verbunden. Die LWL sind in jedem Fall wegredundant auszulegen und auch bei der Gebäudeeinführung und -verteilung weit möglichst zu entflechten.

[2] Die lokalen Netzkopplungen in einer GE mit bspw. einer Kantonspolizei sind zulässig, solange die Netzverbindungen Kanton-Bund noch nicht auf dem neuen optischen Behördennetz Bund (OBNB) aufgesetzt sind.

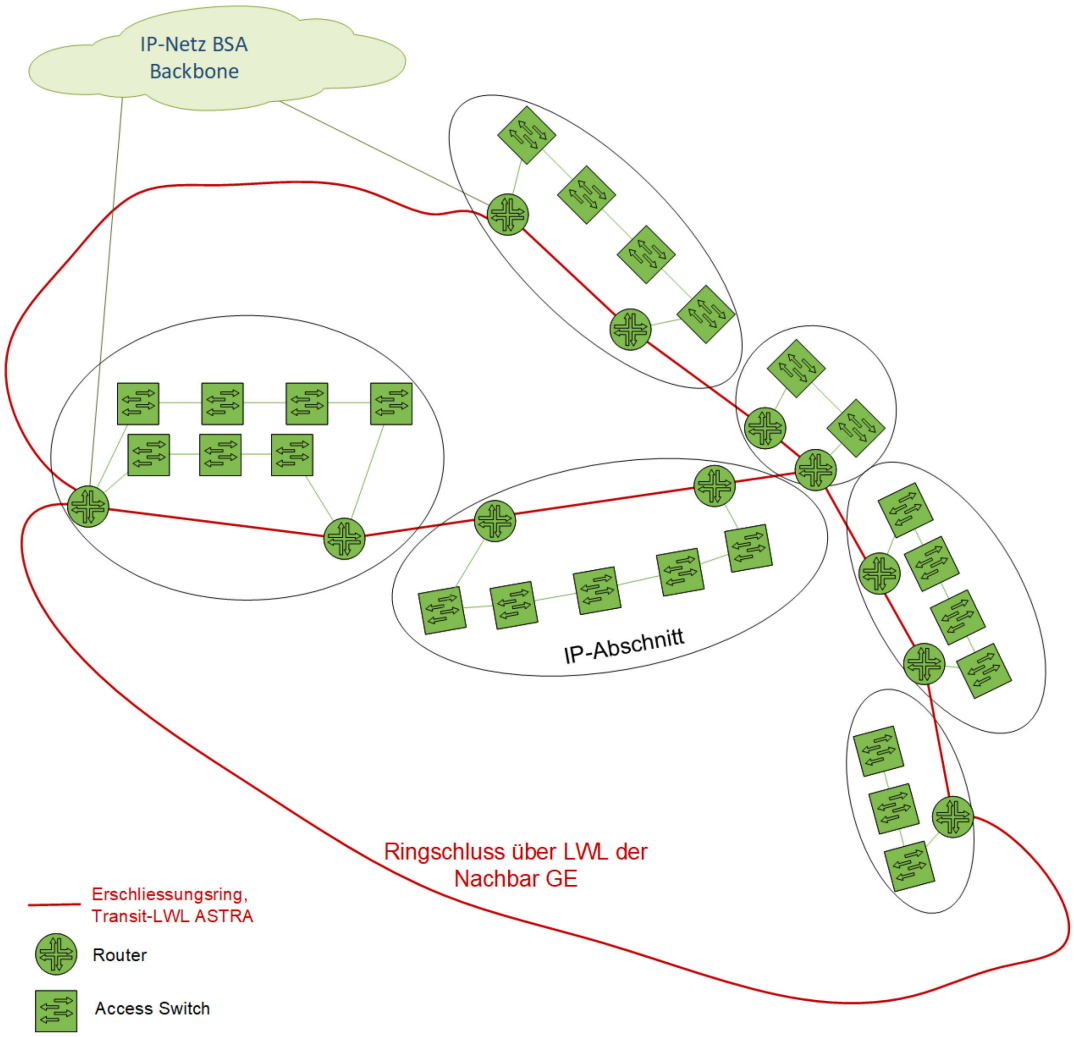

Abb. 2.4 Architektur Erschliessungsringe IP-Netz BSA GE mit den Access-Bereichen

Für den Aufbau der Erschliessungsringe werden die LWL der Transitebene verwendet. Es wird davon ausgegangen, dass genügend Fasern zur Verfügung stehen und i.d.R. keine Mehrfachnutzung einer Faser (WDM Infrastruktur) aufgebaut werden muss. Um die Ringe an der GE-Grenze zu schliessen, stellen sich die GE gegenseitig LWL und Rackspace für optische Komponenten (z.B. Verstärker) bereit.

Alle Perlenketten[3] werden immer an zwei geografisch getrennten Routern angeschlossen. Die beiden Router können dabei sowohl im gleichen Abschnitt (Standard-Design gemäss Abb. 2.5) oder verteilt auf den Abschnitt und seinen Nachbar-Abschnitt (Standard-Design gemäss Abb. 2.6, d.h. ein Router bedient zwei IP-Abschnitte) aufgebaut werden.

[3] Auch mit vielen parallelen Ketten in langen Abschnitten und für grosse Tunnels genügen zwei Router. Der Einsatz von mehr als 2 Routern führt bei Standard-Protokollen wie VRRP oder ERPSv2 zu einem komplexen Design und muss vermieden werden.

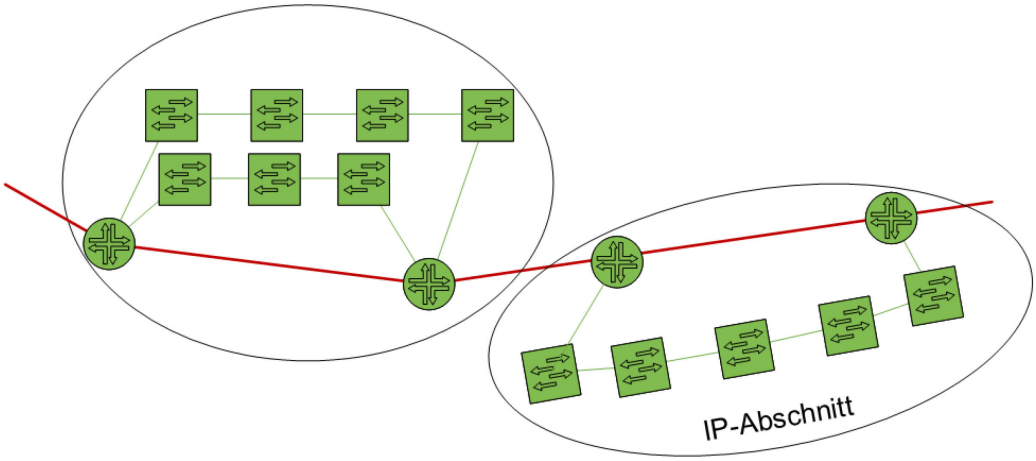

Abb. 2.5 Terminierung Perlenkette: Standard-Design «2 Router im IP-Abschnitt»

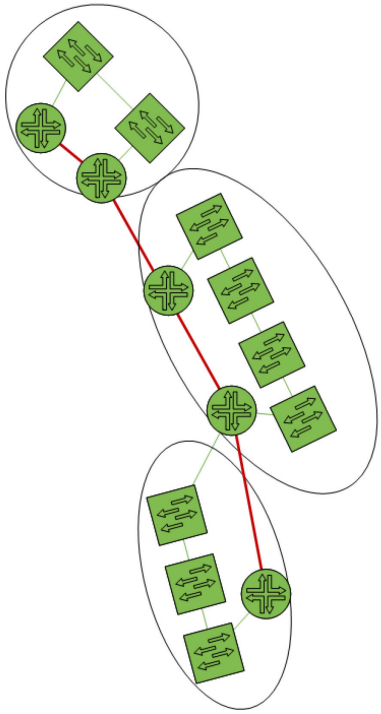

Abb. 2.6 Terminierung Perlenkette: Standard-Design «1 Router im IP-Abschnitt, 1 Router im Nachbarabschnitt»; sinnvoll dort, wo die Platzverhältnisse für einen georedundanten Aufbau im IP-Abschnitt eingeschränkt sind oder wo sehr wenige BSA zu verbinden sind und ein ökonomisches Bauen aus Verfügbarkeitsüberlegungen sinnvoll ist.

2.6 Access im lokalen IP-Abschnitt

Der IP-Abschnitt eines IP-Netz BSA GE bildet den Accessbereich für beispielsweise einen Tunnel, eine offene Strecke oder einen Werkhof. Hier werden sämtliche OT-Systeme der BSA angeschlossen. Der Accessbereich wird künftig bis und mit der Feldebene technologisch einheitlich realisiert, d.h. anlagenspezifische Netzwerklösungen sind auf den Accessbereich zu migrieren.

Der IP-Abschnitt ist als Kaskade traditioneller Access-Switches («Kette», «daisy chain», «Perlenkette») aufgebaut, die an beiden Enden an zwei unterschiedlichen Routern enden. Stichleitungen sind grundsätzlich nicht zugelassen. Innerhalb eines IP-Abschnittes werden nach Bedarf viele dieser Kaskaden parallel gebaut. Die Kaskadierung der Access-Switches erfolgt über die LWL der Objekt- und Feldebene d.h. die Erschliessung soll nicht über die Transit-LWL erfolgen.

Wenn gemäss Standard-Design (Abb. 2.6) ein Ende im Nachbar-Abschnitt terminiert, gehören alle Switches einer Kette immer nur zu einem IP-Abschnitt.

Über diese Switches werden folgende BSA-Systeme angebunden:

- die AR / rVL;
- die AS;
- die LS;
- alle kabelgebundenen IP-fähigen OT-Systeme bzw. OT-Komponenten.

Die Verbindungen zu den oben aufgeführten Komponenten erfolgt über LWL oder Kupferleitungen. Viele moderne OT-Systeme bzw. OT-Komponenten werden dabei über Power over Ethernet (PoE) mit Strom versorgt. Dies ist in den Access-Switches entsprechend vorzusehen. Es dürfen keine separaten PoE Switches eingesetzt werden, sondern die Standard-Access-Switches mit den notwendigen PoE-Modulen bestückt werden.

Lokale proprietäre Netzwerke im Sinne eines LAN auf Ebene Anlage dürfen nicht mehr eingesetzt werden. Stattdessen ist das IP-Netz BSA auch auf der Feldebene zu nutzen, wobei auch dedizierte L2/L3-Dienste (gemäss Abschnitt 3.5) für eine Anlage eingerichtet werden können.

Die Verbindungsregeln zur Vernetzung der Anlagen im Access-Bereich sind in der ASTRA Dokumentation 83045 [9] definiert.

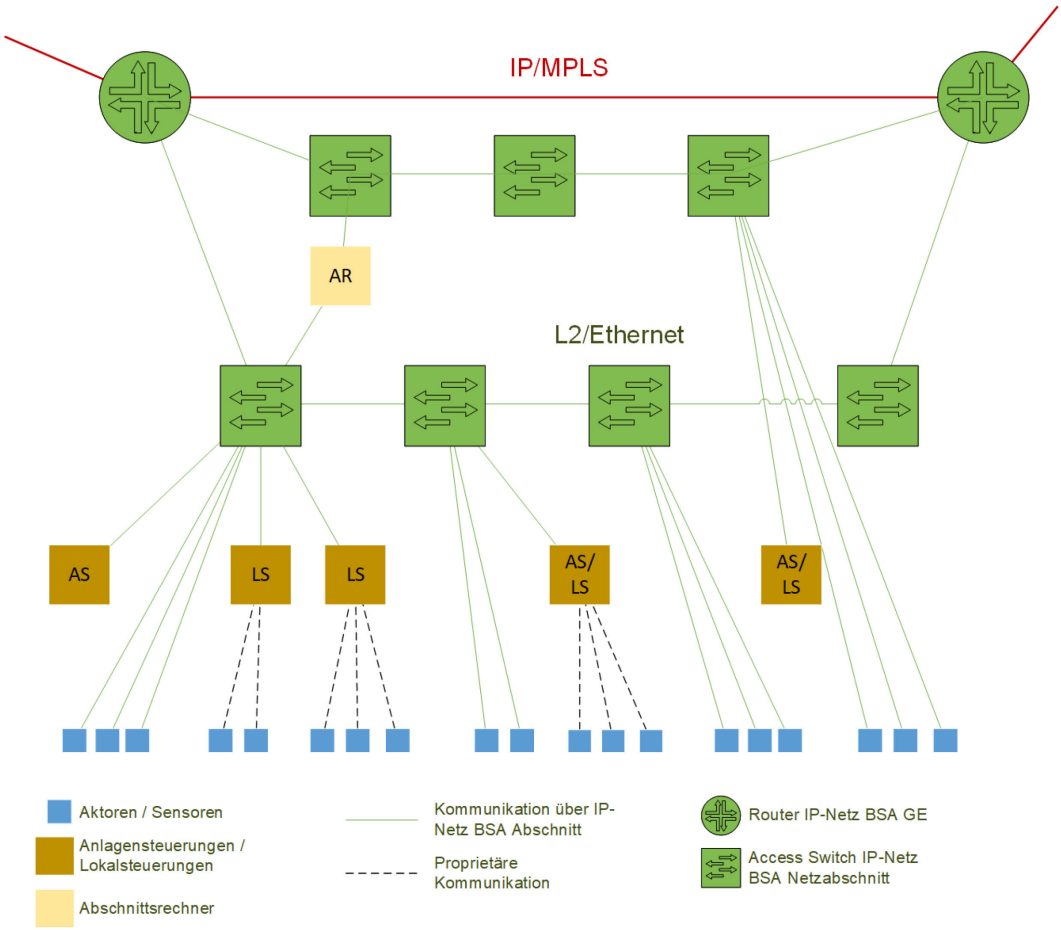

Abb. 2.7 Architektur IP-Netz BSA GE Abschnitt

Die Kaskaden (« Perlenketten ») der Access-Switches werden gemäss folgenden Regeln konzipiert:

- Jede Kaskade («Perlenkette») terminiert am Anfang und am Ende an zwei unterschiedlichen Routern;
- Alle Kaskaden eines IP-Netzes BSA Abschnitt nutzen die gleichen beiden Router (siehe auch Abschnitt 2.5 inkl. Fussnote);
- In einer Kaskade («Perlenkette») dürfen maximal sieben Switches hintereinander gereiht werden. Diese Beschränkung hat zwei Gründe:
  - Laufzeiten bei kritischen Anwendungen sollen ein Maximalmass nicht überschreiten;
  - ein Ausfall bspw. durch Konfigurationsänderungen / Changes auf der Perlenkette kann damit besser auf kurze Teilstücke beschränkt werden.
- Die Endgeräte werden immer an Switches angeschlossen und nicht direkt an Routern;
- In der Realität werden mehrere parallele Kaskaden («Perlenketten») benötigt;
- Zusätzliche Hierarchiestufen, Sub-Switches und der Aufbau getrennter Access-Netze sind nicht zugelassen.

Zur Verdeutlichung werden folgende Beispiele aufgeführt:

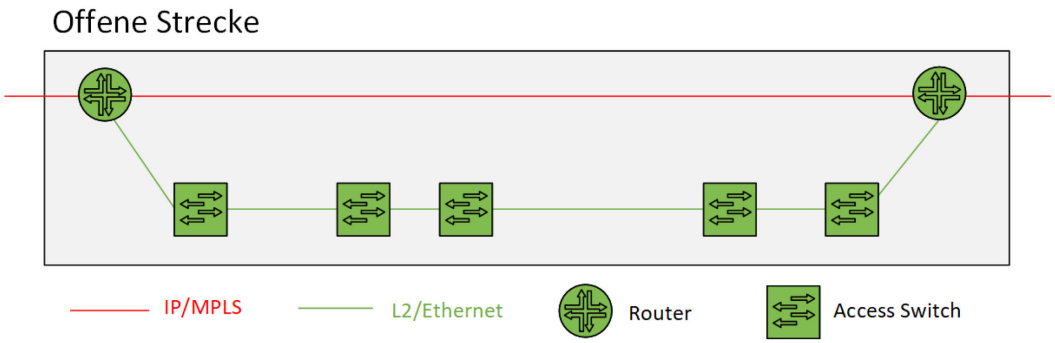

Abb. 2.8 offene Strecke – eine Kaskade («Perlenkette») für beide Fahrtrichtungen

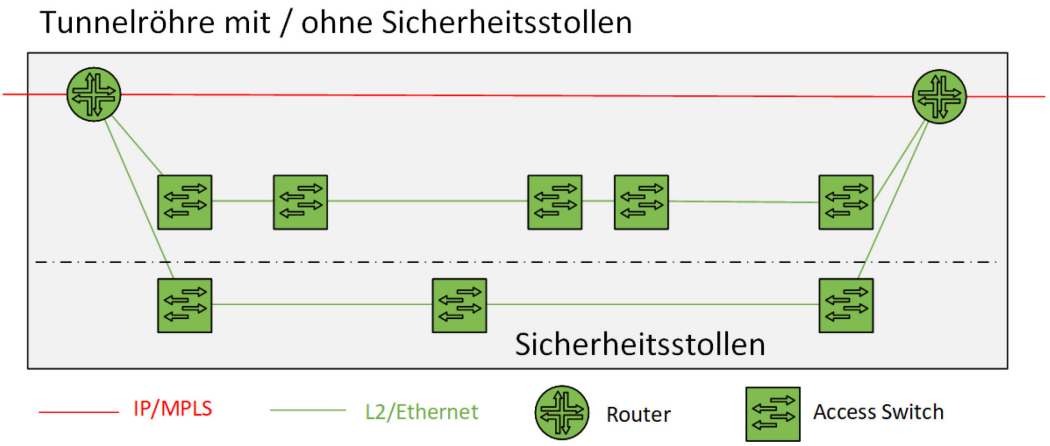

Abb. 2.9 Tunnel – eine Kaskade («Perlenkette») pro Röhre bzw. pro Sicherheitsstollen

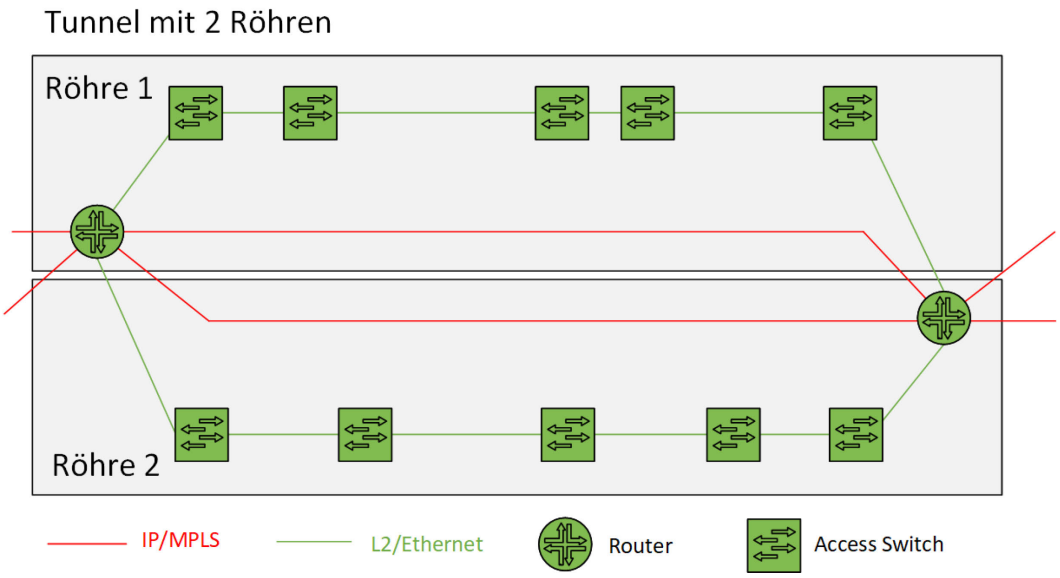

Abb. 2.10 Tunnel mit 2 Röhren – eine Kaskade pro Röhre

Für die Erschliessung von Abschnitten mit vielen Switches sind mehrere Kaskaden notwendig. Da davon ausgegangen wird, dass in einem LWL-Faserbündel (Kabel) genügend freie Fasern zur Verfügung stehen, sind verschiedene Anordnungen der Switches auf unterschiedliche Kaskaden denkbar.

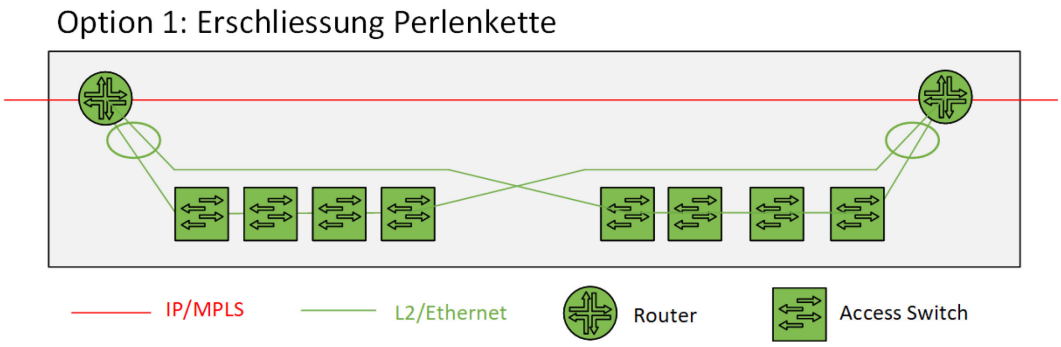

Abb. 2.11 Aufteilung auf mehrere Kaskaden sequentiell angeordnet, Fasern im selben LWL-Kabel

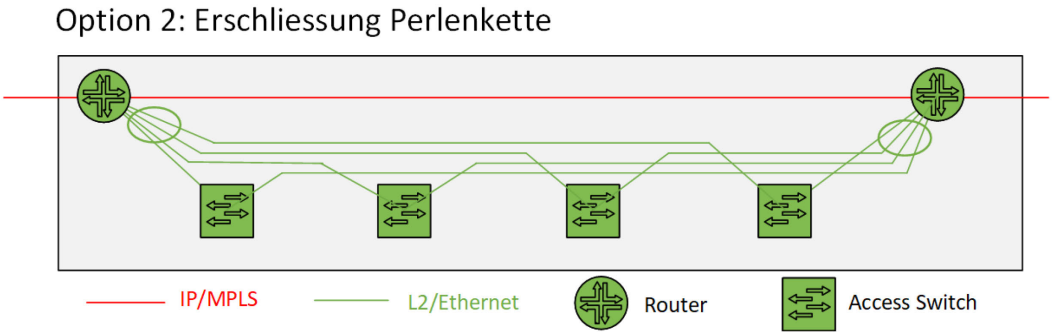

Abb. 2.12 Switches sternförmig angeschlossen, Fasern im selben LWL-Kabel – anstelle eines Switches wie in der Zeichnung, können bis zu 7 Switches angeordnet werden

Mit den aufgeführten Anordnungen lassen sich bspw. Abschnitte mit 28 Switches aufteilen in vier Kaskaden, sequentiell angeordnet und über dasselbe Faserbündel (Kabel) mit vier unterschiedlichen Fasern anbinden.

2.7 Access an zentralen Standorten des IP-Netz BSA GE

Für zentrale Standorte wie Werkhöfe, Data Centers oder Leitzentralen werden ebenfalls IP-Abschnitte definiert und es gelten die gleichen Regeln wie für IP-Abschnitte von Tunnel oder offenen Strecken.

Die IP-Abschnitte werden als Kaskaden traditioneller LAN-Switches («Perlenkette») aufgebaut, die an beiden Enden an zwei unterschiedlichen Routern zur Ringschliessung enden. Innerhalb eines IP-Abschnittes werden mindestens zwei dieser Kaskaden («Perlenketten») gebaut werden, bei Bedarf kann dies natürlich erhöht werden. Damit können die Rechnerinfrastrukturen für die übergeordneten Leitsysteme und weitere OT-Systeme redundant aufgebaut werden.

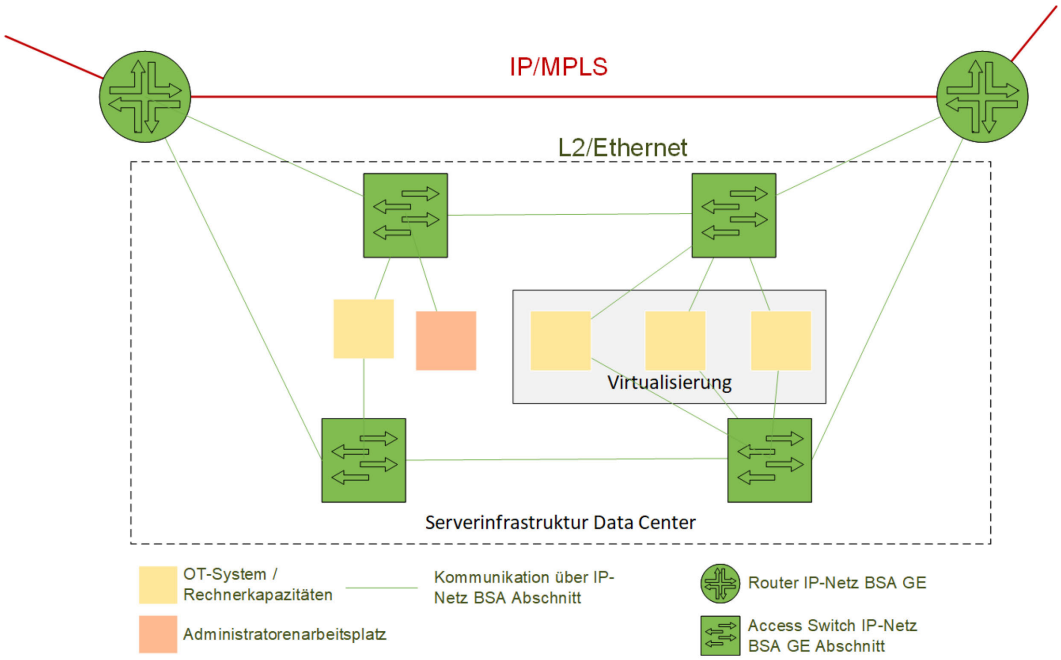

Abb. 2.13 Beispiel-Architektur IP-Abschnitt eines Data Centers

2.8 Nutzung der IP-Netze BSA GE durch Dritte

Fremdgeräte und Fremdnetze dürfen unter Nutzung von transparenten L2-Diensten des IP-Netzes BSA GE erschlossen werden. Dabei ist zwingend ein entsprechendes ISDS-Konzept auszuarbeiten.

Transparente Dienste sind statisch aufgesetzte Punkt-zu-Punkt-Verbindungen, die mit dem IP-Netz BSA der GE keine Kontrolldaten austauschen, sondern das Netz nur zum Transport als «virtuelles Kabel» nutzen. Dies kann rein optisch unter Nutzung von LWL erfolgen oder unter Nutzung von Ethernet Diensten des IP-Netzes BSA GE.

Mögliche Anwendungsbeispiele:

- Radio (DAB): Sendeantennen in Tunnels.

2.9 WLAN

Sollte WLAN im Bereich BSA zugelassen und eingesetzt werden, gibt es aus Netzarchitektursicht keine Einschränkungen.

3 Netzkomponenten IP-Netz BSA

3.1 Allgemeines

Alle eingesetzten Komponenten des IP-Netzes BSA (z.B. Router, Switches, Server, Spannungswandler, Sicherungen, Ventilatoren) müssen den Umgebungsbedingungen am Montagestandort und beim Transport genügen, ohne eine erhöhte Ausfallsrate auszulösen.

Die Netzwerkausrüstung entspricht den physischen Carrier-Anforderungen, wobei im Minimum «NEBS Level 1» gemäss der Telcordia-Normen GR-63-CORE und GR-1089-CORE gefordert wird. «NEBS Level 3» wird angestrebt. Vergleichbare andere Standards (v.a. ETSI und IEC/EN) sind zulässig, solange betreffend Umweltbedingungen (Staub, Temperatur und Feuchte) die Gleichwertigkeit explizit gewährleistet werden kann.

Daneben muss die Ausrüstung den lokalen gesetzlichen Bestimmungen genügen. Im Speziellen sind die Auflagen des Bundes im Bereich «Green IT» bezüglich geringem Energiebedarf zu berücksichtigen.

3.2 Technologie

Als Technologie in den Routern der Erschliessungsringe kommt IP/MPLS oder als Weiterentwicklung Segment Routing[4] (SR) zum Einsatz. Die aktiven Netzwerkelemente der Erschliessungsringe (Router) sind MPLS-Router oder SR-Router, die mindestens mit 25Gbit/s untereinander übertragen. Bei Bedarf soll ein Ausbau auf 100Gbit/s möglich sein.

Die MPLS/SR-Technologie wird nicht in den Access-Bereich ausgeweitet: Als Technologie kommt im Access-Bereich Ethernet-Switching mit virtueller Segmentierung (VLAN) und mit Sicherstellung der Übertragungsqualität und -kapazität (QoS und Policing) zum Einsatz.

Die Ethernet-Switches müssen mit aktivem Management realisiert werden, d.h. sie müssen remote über das NMS administriert und konfiguriert werden können. Einfache Switches ohne Management oder statisch konfigurierte Switches sind nicht zulässig.

Im Access-Bereich werden die Switches mit 10Gbit/s kaskadiert. Im Bedarfsfall werden mehrere Schnittstellen zur Bandbreitenerhöhung gebündelt (Ethernet-LAG). Der Einsatz von 100Gbit/s im Access-Bereich ist nicht vorgesehen.

3.3 Innere Redundanz Netzwerkkomponenten

Unter innerer Redundanz wird die redundante Ausführung von Stromversorgung, Controller-Karten und Interface-/ Netzwerk-Karten verstanden. Sie schützt gegen den Ausfall einer einzelnen Baugruppe des Netzwerkgerätes oder eines Stranges der Versorgung.

Die Geräte werden bewusst einfach gehalten und es gelten folgende Anforderungen sowohl für Router als auch für Switches:

- Eine innere Redundanz der aktiven Komponenten (z.B. zwei Kontroller-Karten, zwei Netzwerkschnittstellen) oder zwei getrennte Geräte werden nicht gefordert;

[4] Als Weiterentwicklung des MPLS sind beim Segment Routing alle Varianten wie SRv6 oder SR-MPLS gleichermassen zulässig. Einfache, konsistente Protokolle könnten gegenüber IP/MPLS einen Vorteil darstellen.

- Eine zweistrangige (redundante) Stromversorgung wird angestrebt, ist aber nur bei den MPLS-Routern zwingend und im Access-Layer dort, wo auch die angeschlossenen BSA-Systeme eine zweistrangige Stromversorgung aufweisen.

3.4 Netzwerkschnittstelle (NNI, Network-Network Interface)

3.4.1 Backbone-NNI

Für die Schnittstelle zum Backbone, die zur Verbindung zu den anderen GE, den RZ und der VMZ-CH dient, ist die Funktionalität bewusst geringgehalten. Die Schnittstelle ist aber auf eine hohe Bandbreite ausgelegt, um mit den erwarteten künftigen Entwicklungen ohne Änderungen Schritt halten zu können.

Die Netzschnittstelle für das Backbone-NNI wird im Detail durch den Dienstleister des Bundes bestimmt. Die bekannten übergeordneten Eigenschaften sind wie folgt:

- Physikalisch ist das Backbone-NNI Ethernet-basiert. Pro Standort kommt eine einzelne 10GBit/s-Schnittstelle zum Einsatz. Eine Bündelung oder höhere Schnittstellengeschwindigkeiten kommen für höhere Bandbreiten zum Einsatz;
- Die Backbone-NNI-Schnittstelle überträgt den gesamten Nutzverkehr ohne logische Unterteilung aber mit Priorisierung in einem einzigen L3-VPN;
- Zur direkten Überwachung der Konnektivität durch die GE muss das Ethernet-CFM (Connectivity Fault Management gemäss 802.1ag/Y.1731) unterstützt werden;
- Für den Bezug der einheitlichen Zeit- und Taktinformation muss Synchrones Ethernet mit den entsprechenden Funktionen (Precise Timing Protocol gemäss IEEE 1588) verfügbar sein;
- Eine Verschlüsselung wird nicht gefordert.

Aus Sicht des IP-Netzes BSA GE erscheint das Backbone-NNI als externes Interface, d.h. weder die MPLS-spezifischen Protokolle noch die allgemeinen Routing-Protokolle zum internen Topologie-Austausch sind aktiviert. Zur Optimierung der Betriebsprozesse wird aber von einer rein statischen Routing-Konfiguration abgesehen. Auf der Backbone-NNI-Schnittstelle werden mittels eBGP automatisiert die Topologie zwischen den GE, BD, den RZ und der VMZ-CH abgeglichen.

3.4.2 Router-NNI

Zwischen den Routern einer GE, die die Abschnitte untereinander verbinden und die WAN-Konnektivität innerhalb der GE sicherstellen, erfolgt die Kommunikation über das Router-NNI.

Die Netzschnittstelle für das Router-NNI ist wie folgt spezifiziert:

- Physikalisch ist das Router-NNI Ethernet-basiert. Es kommt eine einzelne 25/40GBit/s-Schnittstelle zum Einsatz, die (möglichst) ohne optische Verstärkung über die LWL der GE geführt sind;
- Für den Austausch der einheitlichen Zeit- und Taktinformation muss Synchrones Ethernet mit den entsprechenden Funktionen (Precise Timing Protocol gemäss IEEE 1588) verfügbar sein;
- Eine Verschlüsselung wird nicht gefordert;
- Die Router-NNI-Schnittstelle unterstützt die logische Unterteilung der Schnittstelle mit MPLS oder SR;
- Auf der Router-NNI-Schnittstelle sind sowohl die Protokolle für die MPLS/SR-Topologie (z.B. IS-IS, LDP und RSVP) wie auch für die IP-Topologie aktiviert. Die zu verwendenden Protokolle sind nicht verbindlich vorgeschrieben, müssen aber sämtliche Netzwerkdienste effizient unterstützen.

3.4.3 Access-Uplink (Access-NNI)

Zwischen den Routern und dem Access, der als einfach Layer-2-Struktur ohne MPLS/SR realisiert ist, definiert der Access-Uplink das Zusammenspiel an der Schnittstelle der beiden Netzwerkbereiche.

Die Netzschnittstelle für den Access-Uplink ist wie folgt spezifiziert:

- Physikalisch ist der Access-Uplink Ethernet-basiert. Es kommt eine einzelne 10GBit/s-Schnittstelle oder 1GBit/s-Schnittstelle zum Einsatz, die ohne Verstärkung oder Signal-Regenerierung über die LWL der GE geführt sind;
- Eine Verschlüsselung wird nicht gefordert;
- Die Schnittstelle unterstützt die logische Unterteilung der Schnittstelle (mittels VLAN gemäss 802.1Q und QinQ gemäss IEEE 802.1ad);
- Für Management- und Kontrollaufgaben sind logische Netze (VLAN) definiert;
- Der Access-Uplink ist eine reine Layer-2-Schnittstelle ohne Routingprotokolle;
- Die Redundanz-Umschaltung der zweifachen Anbindung am zwei Routern. Für diese Umschaltung kommt Shortest Path Bridging (SPB gemäss IEEE 802.1aq) oder Ethernet Ring Protection Switching (ERPSv2 gemäss ITU-T G.8032 mit CFM) zum Einsatz[5].

Das Mapping der logischen Netzstrukturen (inkl. QoS) in den Erschliessungsringen (mittels MPLS oder SR) auf die logischen Netzstrukturen im Access (mittels VLAN) übernimmt der Router. Er terminiert seine logischen Netzstrukturen (L2/L3-Dienste) und stellt sie als Layer-2-Verlängerung den Access-Switches zu Verfügung. Die Router agieren bei L3-Diensten als VRRP-Instanzen, um Redundanz sicherzustellen, ohne dass angeschlossene Endgeräte oder die Access-Switches spezielle Protokolle unterstützen müssen.

3.5 Benutzerschnittstelle (Userport)

Die Schnittstelle ist immer eine Ethernet-Schnittstelle, wobei ein Anschluss über Kupfer-Kabel oder Singlemode-LWL mit Geschwindigkeiten bis 10Gbit/s möglich ist. Als Service-Schnittstelle kann sowohl die gesamte physikalische Schnittstelle, oder eine logische VLAN-Schnittstelle darauf (gemäss IEEE 802.1Q) genutzt werden. Für Endgeräte ausserhalb der Serverräume ist 1000Base-T der Standard für galvanische Schnittstellen und 1000Base-LX der Standard für optische Schnittstellen.

In den Serverräumen sind zusätzlich optische 10GE-Schnittstellen (10GBASE-LR) und Multigigabit galvanische Schnittstellen vorzusehen.

Das IP-Netz BSA der GE unterstützt nur Ethernet-basierte Dienste. Sogenannte Legacy-Dienste, wie E1-Mietleitungen oder RS-232, werden nicht angeboten.

Folgende Netzdienste sind innerhalb der GE verfügbar.

Ethernet-Dienste («L2-Dienste»):

- Punkt-Punkt-Verbindung zwischen zwei Ports (Virtual Leased Lines, VLL);
- Verteilter Layer-2-Switch mit Kommunikation von vielen Ports zu einem Sternpunkt aber ohne direkte Kommunikation untereinander (Ethernet Virtual Private Tree oder E-Tree);
- verteilter Layer-2-Switch mit Kommunikation zwischen vielen Ports ohne Einschränkung (Ethernet Virtual Private LAN oder E-LAN).

[5] Nur zur Anbindung von nicht-migrationsfähigen Legacy-Access-Bereichen, wo die Layer-2-Switches nicht getauscht werden können, ist das Spanning-Tree-Protokoll (STP gemäss IEEE 802.1D, 802.1w oder 802.1s) zulässig.

IPv6-Dienste («L3-Dienste mit IPv6»):

- Multipunkt-Punkt « Hub-and-Spoke» (viele Aussenpunkte zu einem Sternpunkt);
- Multipunkt-Multipunkt «Any-to-Any» (geografisch verteilter virtueller Router).

IPv4-Dienste («L3-Dienste mit IPv4»):

- Multipunkt-Punkt « Hub-and-Spoke» (viele Aussenpunkte zu einem Sternpunkt);
- Multipunkt-Multipunkt «Any-to-Any» (geografisch verteilter virtueller Router).

Dualstack IP-Dienste («L3-Dienste mit IPv6 und IPv4»):

- Multipunkt-Punkt « Hub-and-Spoke» (viele Aussenpunkte zu einem Sternpunkt);
- Multipunkt-Multipunkt «Any-to-Any» (geografisch verteilter virtueller Router).

GE-übergreifende Netzwerkdienste über das/den IP-Netz BSA Backbone sind nicht mittels MPLS oder SR direkt umsetzbar.

3.6 QoS/Bandbreiten per SLA

Grundsätzlich stehen jedem Dienst die per SLA[6] garantierte Bandbreite («comitted information rate») zur Verfügung. Wird dieser Wert nicht überschritten, sind sowohl Laufzeiten wie auch die Varianz der Laufzeit («Jitter») minimal (Laufzeit unter 10 ms, Varianz unter 2 ms). Die Paketverlustrate ist weniger als 10^{-6}.

Für Dienste, deren Verkehr stark variiert und wo die Laufzeit und ggf. Paketverluste weniger kritisch sind, kann eine zusätzliche Bandbreite («peak information rate») im SLA hinterlegt werden. Bis zu dieser höheren Rate versucht das IP-Netz BSA GE die Daten zu übertragen oder temporär zu speichern.

Die genauen Werte sind pro GE im SLA spezifiziert, da speziell die Laufzeiten von der geografischen Ausdehnung des IP-Netzes BSA GE abhängt.

3.7 Härtung

Die Härtung der Netzwerkkomponenten erfolgt grundsätzlich gemäss den Vorgaben der Richtlinie ASTRA 13030 «IT-Sicherheit der Leit- und Steuersysteme BSA» [2].

[6] SLA = Service Level Agreement. Es wird davon ausgegangen, dass für jeden benötigten Dienst eine Spezifikation vorliegt, die die Anforderungen an das Netz beinhaltet.

3.8 Zeit- und Taktverteilung

Alle Netzwerkelemente des IP-Netzes BSA in den Erschliessungsringen unterstützen PTP und SyncE zur Verteilung präziser Zeit- und Taktinformation über NNI-Schnittstellen. Das IP-Netz BSA Backbone überträgt SyncE und PTP von den beiden Standorten der Basisdienste zu allen Teilnetzen im IP-Netz BSA.

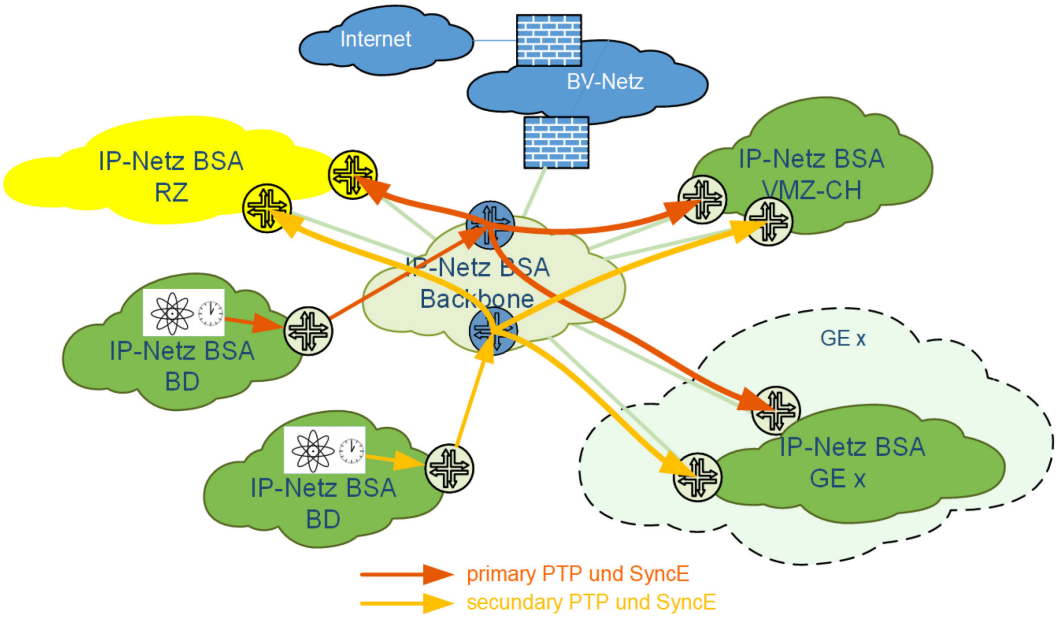

Abb. 3.14 Nationale Verteilung von Zeit und Takt über das IP-Netz BSA Backbone

Über die NNI-Schnittstellen der Router im IP-Netz BSA der GE, VMZ oder RZ verteilen die Netzwerkelemente der Erschliessungsringe die Takt- und Zeitinformation innerhalb der Teilnetzte.

Die Zeitinformation wird von allen angeschlossenen Systemen, den Netzwerkelementen des Access-Layers und den Endsystemen über NTP (oder künftig PTP) bezogen. Die Taktinformation kann bei Bedarf an den Routern der Erschliessungsringe im Abschnitt abgegriffen werden. Weder SyncE noch PTP müssen von den Netzwerkelementen im Access-Layer unterstützt sein.

Wegen der Schaltsekundenproblematik muss intern in allen Netzwerkelementen mit TAI (Temps Atomique International) anstelle der UTC (Universal Time, Coordinated) gearbeitet werden.

Die ASTRA Dokumentation 83044 [7] beschreibt die Umsetzung.

4 IP-Netz BSA Backbone

Das IP-Netz BSA Backbone ist ein vom BIT (Bundesamt für Informatik und Telekommunikation) betriebener IP-Backbone, welcher auf einem von der FUB (Führungsunterstützungsbasis) betrieben optischen Transportnetzwerk (optisches Behördennetz Bund, OBNB) basiert. Zur Vernetzung der optischen Knoten (WDM-Infrastruktur) im OBNB werden LWL des ASTRA (entlang der Nationalstrasse) sowie LWL der FUB (Führungsnetz CH) eingesetzt.

Das IP-Netz BSA Backbone wird nach einer «Hub & Spoke» Topologie aufgebaut. Mit dem Backbone werden die 11 Gebietseinheiten (GE), die Verkehrsmanagementzentrale (VMZ-CH) sowie die Rechenzentren der Betriebs- und Sicherheitsausrüstung (RZ BSA A/B) und die Basisdienste IP-Netz BSA (BD A/B) vernetzt.

Pro GE, VMZ-CH und RZ BSA werden je zwei Standorte (A und B-Standorte) als Spoke-Site realisiert. Als Hub-Sites werden die zivilen Standorte des RZ Verbundes (RZ PRIMUS und RZ CAMPUS) genutzt. Sofern der Datenverkehr den IP-Netz BSA Backbone nicht verlässt, wird der Verkehr einer Spoke-Site jeweils via Hub-Site an eine andere Spoke-Site übermittelt. Verlässt der Datenverkehr den IP-Netz BSA Backbone, erfolgt dies entweder über einen Ausgang an der Spoke-Site, vorzugsweise über die Standorte Basisdienste (z.B. Datenverkehr ASTRA zu kantonalem Polizeikorps) oder über die Hub-Site (z.B. Datenverkehr zu anderen Netzzonen des Bundes).

5 IP-Adressierung

5.1 Grundsätze

Alle fest installierten Geräte, welche an das IP-Netz BSA angeschlossen werden, sind mit fixen Adressen versehen. Dabei wird im gesamten IP-Netz BSA das IP-Protokoll in der Version 6 (IPv6) verwendet. Die Verwendung von IPv6 zur Adressierung von Netzelementen und zum Aufbau der IP/MPLS Subnetze ist zwingend. Das IP-Netz BSA selbst muss IPv4/IPv6 Dualstack-fähig sein.

Die Kommunikation auf der Managementebene, auf der Ebene Region (BLZ/ELZ/UeLS) und auf der Abschnittsebene (AR/rVL/AS) muss IPv6 nutzen.

Da verschiedene Geräte auf Feldebene (LS/Aktoren/Sensoren) IPv6 nicht unterstützen, ist es im Ausnahmefall erlaubt, weiterhin das IPv4-Protokoll für die Kommunikation zwischen diesen Geräten zu nutzen. Da die IPv4-Adressierung in den lokalen Subsystemen bereits gegeben ist, wird in diesem Kapitel nur das IPv6-Adresskonzept beschrieben, welches für jegliche Geräte im IP-Netz BSA gilt.

5.2 IPv6-Adresskonzept

Erklärungen zum IPv6-Adressformat werden hier nicht aufgeführt und können dem RFC 4291 entnommen werden.

Es gelten folgende Grundsätze für die IPv6-Adressstruktur:

- Es wird angenommen, dass das ASTRA nur eine Domäne (nationalstrassen.admin.ch) betreibt, und der vom Bund zugewiesene Adressbereich vollständig für diese Domäne verwendet werden kann;
- Der vom Bund (Bundeskanzlei) dem ASTRA zur Verfügung gestellte IPv6-Adressbereich lautet:
  - **2a07:2900:8000::/40**
- Der IPv6-Adressaufbau basiert auf der Grundarchitektur IP-Netz BSA, den BSA-Abschnitten gemäss SA-CH und der Netzwerkzonierung IP-Netz BSA.

5.3 Netz- und Host-Teil der IPv6 Adresse

Die 128 Bit einer IPv6-Adresse sind in einen Netz-Teil (erste 64 Bit) und einen Host-Teil (letzte 64 Bit) aufgeteilt und werden für das IP-Netz BSA wie folgt definiert:

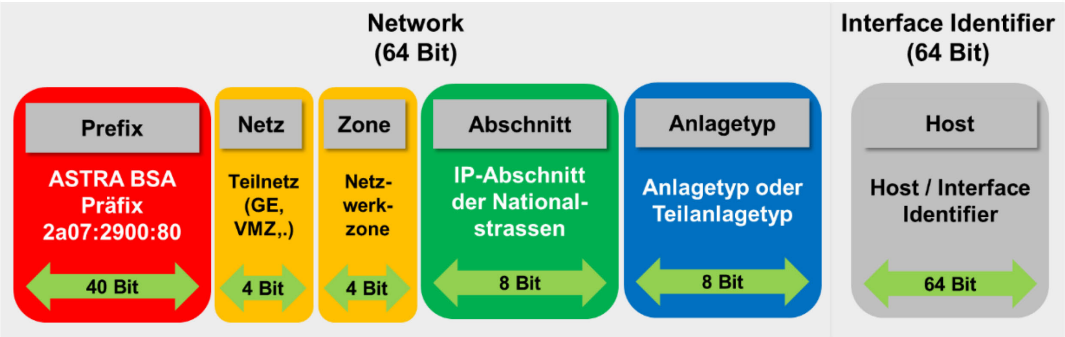

Abb. 5.1 IPv6-Adressstruktur

Der Netz-Teil der IPv6-Adresse ist wie folgt aufgebaut:

Namen	Länge	Bemerkung
Prefix	40 Bit	Vorgegebenes Präfix des Bundes
Netz	4 Bit	Teilnetz (IP-Netz BSA GE/VMZ-CH/...)
Zone	4 Bit	Netzwerkzone (Prozesszone, Managementzone, …)
IP-Abschnitt	8 Bit	IP-Abschnitt
Anlage	8 Bit	Subnetz («VLAN») einer bestimmten Anlage/Teilanlage in Anlehnung an 13013 AKS-CH Aspekt Produkt, Gliederungsebenen 1 und 2: Die IPv6-Struktur teilt die Betriebs- und Sicherheitsausrüstungen in teilanlage- oder anlagebezogene Subnetze auf. D.h. in jedem BSA Abschnitt verwalten i.d.R. die beiden Abschnitts-Router für jede Anlagesteuerung ein eigenes Teilnetz.
Host	64 Bit	Die Hostadresse bzw. Interface Identifier Adresse ist frei wählbar.

Fig. 5.2 Adressstruktur IPv6

Details werden in der ASTRA Dokumentation 83040 IP-Adressierung geregelt [3].

6 DNS, DHCP und IP Address Management

6.1 IP-Adressverwaltung

Für die Verwaltung von IPv4/v6-Adressen gelten folgende Regeln:

- Die Verwaltung der IPv4- und der IPv6-Adressen muss über das zentrale IPAM/DDI-Tool erfolgen;
- Es muss DNS für die Zuweisung von Hostnamen zu Adressen genutzt werden. Jeder Host muss eindeutig über seinen DNS-Namen identifizierbar sein;
- Der Zugriff auf Geräte muss grundsätzlich immer über den Hostnamen möglich sein. Dies gilt insbesondere für Zugriffe von Endgeräten für Enduser auf Geräte. In Ausnahmefällen kann der Zugriff direkt über IP-Adressen erfolgen;
- Da im Regelfall Hostnamen in die Konfiguration eines Verbindungsaufbaus aufgenommen werden, muss sichergestellt werden, dass diese immer zu einer Adresse aufgelöst werden können. Dies erfolgt über den DNS-Server oder über das Hostfile auf dem Endgerät;
- Im Falle der Auflösung über den DNS Server muss die Erreichbarkeit des DNS Servers immer sichergestellt werden;
- Im Falle einer Auflösung über das Hostfile muss sichergestellt werden, dass das Hostfile immer mit den Inhalten des DNS-Servers übereinstimmt, welcher für die Zuteilung von Hostnamen zu Adressen massgebend ist.

6.2 IPAM/DDI-Architektur

DNS Services, DHCP Services und IP Address Management sind eng miteinander verknüpft. Damit das Verwalten der notwendigen Services effizient und möglichst fehlerfrei erfolgen kann, muss ein integriertes DNS, DHCP und IPAM Tool (IPAM/DDI-Tool) verwendet werden.

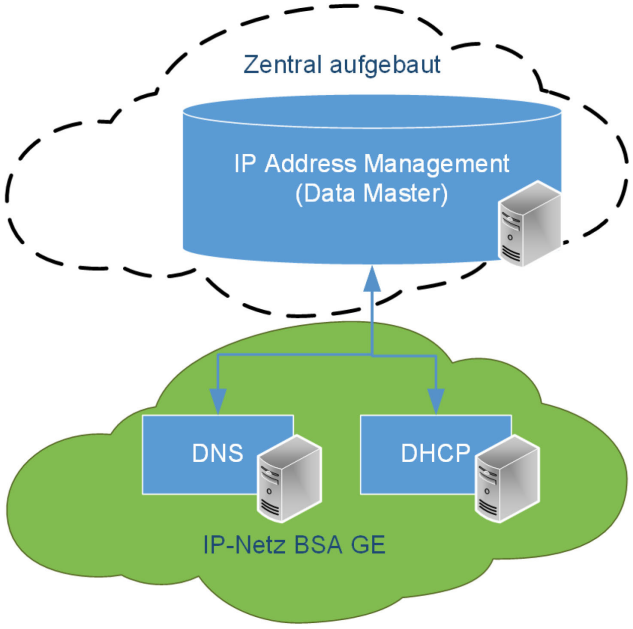

Abb. 6.1 Architektur IPAM/DDI

Das IPAM/DDI-Tool (Data Master) für die Verwaltung der IP-Adressen wird zentral aufgebaut. Über das IPAM/DDI-Tool werden sowohl DNS- als auch DHCP-Services konfiguriert. Die DNS- und DHCP-Server werden redundant in den GE aufgebaut bzw. weiterverwendet, soweit die vorhandene Infrastruktur durch das IPAM-Tool administriert werden kann.

6.3 Anforderungen an das IPAM/DDI-Tool

An das IPAM/DDI-Tool werden folgende Anforderungen gestellt:

- **Automatisiertes IP-Adressmanagement**
  Es muss möglich sein, IP-Adressen automatisch zu scannen und damit eine aktuelle Bestandsliste der verwendeten und freien IP-Adressen zu erstellen. Dabei muss es möglich sein, sowohl IPv4 als auch IPv6 Adressen bzw. Adressblöcke auf demselben Netzwerk zu verwalten.
- **Integrierte DHCP- und DNS-Verwaltung**
  Über eine zentrale Konsole sollen DHCP-Reservierungen und DNS-Einträge verwaltet werden können. Damit entfällt die individuelle Datenadministration lokal auf den unterschiedlichen DHCP- und DNS-Servern.
- **Erkennen von IP-Konflikten**
  Das IPAM/DDI-Tool soll IP-Konflikte, erschöpfte Subnetze/Bereiche oder abweichende DNS-Einträge melden und entsprechende Alarme oder Reports generieren.
- **Verwaltung delegieren**
  Es muss möglich sein, die Verwaltung von bestimmten IP-Adressbereichen und Aufgaben an unterschiedliche Rollen zu delegieren. Die GE müssen ihre Adressbereiche eigenständig bearbeiten und die Administration von DNS und DHCP eigenständig durchführen können.

6.4 Aufbau und Betrieb IPAM/DDI-Tool

Die ASTRA Dokumentation 83041 [4] wird den Aufbau und den Betrieb des IPAM/DDI-Tools regeln.

7 Security und Netzwerkzonen

Für die Security im IP-Netz BSA gelten die Anforderungen aus der Richtlinie ASTRA 13030 [2].

Neu ist ein Netzwerkzonenmodell gemäss den Vorgaben des Bundes umzusetzen (Si001 – IT-Grundschutz in der Bundesverwaltung vom 01. März 2022). Das Zonenmodell IP-Netz BSA ist angepasst auf die Bedürfnisse der BSA und wird in der ASTRA Dokumentation 83042 Network Security Policy (NSP) IP-Netz BSA [5] beschrieben. Die Dokumentation regelt den Aufbau und den Betrieb der Netzwerkzonen und beschreibt die technischen und betrieblichen Massnahmen.

8 Network Access Control (NAC)

Der Anschluss von Geräten auf dem IP-Netz BSA wird in der der ASTRA Dokumentation 83042 Network Security Policy (NSP) IP-Netz BSA [5] geregelt und ist Teil von verschiedenen Massnahmen zur Erhöhung der Sicherheit im IP-Netz BSA. Auf ein spezifisches Network Access Control System (NAC) als eigenständiges System wird verzichtet.

9 Network Management System (NMS)

Zur Verwaltung und Betriebsüberwachung eines IP-Netzes BSA GE muss ein Netzwerkmanagementsystem (NMS) eingesetzt werden[7]. Die Aufgaben des NMS werden zusammengefasst unter dem Begriff FCAPS[8]:

- F: *Fault Management* (Fehlermanagement);
- C: *Configuration Management* (Konfigurationsmanagement);
- A: *Accounting Management* (Administration Management);
- P: *Performance Management* (Leistungsmanagement);
- S: *Security Management* (Sicherheitsmanagement).

9.1 Fault Management (Fehlermanagement)

Das Fehlermanagement ist zusammen mit dem Konfigurationsmanagement der wichtigste Teil des Netzwerkmanagements. Es sollen Fehler frühzeitig erkannt und dadurch die Verfügbarkeit des Netzwerkes erhöht werden.

Spezifische Anforderungen an das Fault Management:

- Durchgängiges end-to-end Monitoring aller Netzdienste innerhalb des IP-Netzes BSA GE;
- Monitoring aller Netzkomponenten und Medien (LWL-Strecken) innerhalb des IP-Netzes BSA GE;
- Echtzeit-Visualisierung des Netzwerkes (logisch und physikalisch);
- Alarme von physischen oder logischen Komponenten müssen Netzdiensten zugeordnet werden können;
- Alarme müssen korreliert werden und Folgealarme durch eine leistungsfähige Analyse (Root-Cause-Analyse) ausgeblendet werden können. Die Root-Cause-Analyse muss nahtlos über das gesamte Netz möglich sein;
- Fehlerzusammenhänge müssen aufgezeigt werden, eine schnelle Navigation von Alarm zu Ursache und betroffenen Elementen und Services muss vorhanden sein;
- Alarme müssen klassifiziert und gefiltert werden können;
- Mehrerer Alarmwindows müssen gleichzeitig aktiv sein können;
- Aus den Alarmwindows muss eine direkte Navigation zu den auslösenden/betroffenen physischen Objekten (Gerät/Port) und logischen Objekten (Services) möglich sein;
- Fehler müssen 12 Monate archiviert werden und in dieser Zeit im GUI visualisierbar bleiben (Protokollieren von Fehlern).

9.2 Accounting Management (Administration Management)

Da die IP-Netze GE nicht abgerechnet werden, wird der Begriff Administration statt Accounting verwendet. Administration enthält die Verwaltung von Benutzern, Passwörtern und Zugriffsberechtigungen.

---

[7] Wenn bestimmte Funktionen außerhalb des NMS realisiert werden müssen oder bereits verfügbar sind, ist dies explizit erlaubt, sofern die erforderliche Funktionalität gewährleistet werden kann. Beispiel: Es ist erlaubt, die Aufzeichnung der Zugriffe eines Administrators über ein dediziertes Logging-System zu realisieren.

[8] gemäss ISO/IEC 7498-4: Information Processing Systems -- Open Systems Interconnection -- Basic Reference Model -- Part 4: Management Framework

Spezifische Anforderungen an das Administration Management:

- Verwaltung der Benutzerrechte (Zugriff, Limits und Prioritäten) für Netzwerkkomponenten wie Router, Switch, etc.;
- Rollenmodell mit entsprechenden Zugriffsrechten muss unterstützt werden;
- Zugriffsrechte müssen sowohl auf funktionaler Ebene als auch auf den Zugriff auf bestimmte Netzelemente gesetzt werden können (bspw. sollen Nutzer nur eigene Elemente sehen können);
- Protokollierung.

9.3 Configuration Management (Konfigurationsmanagement)

Das Configuration Management umfasst alle Funktionen im Zusammenhang mit der Konfiguration des Netzes und den Netzkomponenten.

Spezifische Anforderungen an das Configuration Management:

- Konfiguration von Hardware-Elementen wie bspw. Network Interfaces, Ports etc. Das Konfigurieren eines Netzelementes via Command Line Interface (CLI) des Netzelementes ist nur im Ausnahmefall gestattet;
- Konfigurationen von neuen Netz-Services müssen mittels einfachen grafischen end-to-end Operationen ausgeführt werden können. Entsprechende vordefinierte und anpassbare Templates müssen zur Verfügung stehen (Dienst bzw. Templates auswählen, Endpunkte auswählen, Überprüfung und automatische Provisionierung des primären und auch sekundären Pfades);
- Ebenso gehört dazu, dass bspw. beim Ersatz von Netzwerkkomponenten Kopier-funktionen zur Verfügung stehen, um bestehende Konfigurationen schnell zu übernehmen und anzupassen;
- Simulation und Verifikation von Konfigurationen, Anzeige der Bandbreitennutzung auf jedem Pfad und physischen Link;
- Traffic Shaping (Analyse des Netzwerkes, Optimierung des Netzwerkes);
- Alle Netzwerkgeräte müssen inventarisiert werden können:
  - Router, Switches;
  - Leitungen, Netzanschlüsse;
  - Gateways.
- Versionsverwaltung der Konfigurationen und der Software pro Gerät.

9.4 Performance Management (Leistungsmanagement)

Im Leistungsmanagement werden quantitative Messresultate verarbeitet um qualitative Aussagen machen zu können.

Spezifische Anforderungen an das Performance Management:

- Bandbreiten (vorgehaltene auf redundanten Pfaden und effektiv genutzte) müssen dargestellt werden können;
- Paketverlust, Laufzeiten und dessen Varianz etc. müssen überwacht werden können
- Veränderungen dieser Grössen müssen über beliebige Zeitfenster ausgewiesen werden können;
- Alarme bei Grenzwertüberschreitungen müssen unterstützt werden können;
- Statistiken müssen in grafischer und tabellarischer Form verfügbar sein;
- Reports müssen nach MS-Office exportiert werden können (CSV, XLSX, DOCX).

9.5 Security Management (Sicherheitsmanagement)

Das Sicherheitsmanagement kontrolliert und schützt die Zugriffsberechtigung auf Netzwerkdaten.

Spezifische Anforderungen an das Security Management:

- Sämtliche Aktivitäten sowohl von Benutzern als auch von extern verbundenen Systemen müssen geloggt werden;
- Die Auditfähigkeit muss systemweit gewährleistet sein. Insbesondere müssen Ereignisse wie physische Eingriffe an der Ausrüstung sowie Zugriffe via CLI oder lokales Terminal in den Logs sichtbar sein.

10 Betrieb

10.1 Standard Service Levels

Die Anforderungen an den Betrieb IP-Netz BSA und ihrer operativen Support-Systeme werden über standardisierte Service Levels definiert.

10.1.1 Servicezeit

Die **Servicezeit** definiert die Zeit, in welcher die Service-Erbringung vereinbart ist. Der am Service Access Point gelieferte Service wird proaktiv oder reaktiv überwacht.

Die **Wartungszeit** (Wartungsfenster) umfasst die mit diesem Service Level Parameter vereinbarte Zeit, in der Wartungsarbeiten für einen Service durchgeführt und geplant keine Serviceleistungen erbracht werden.

Messgrösse	Wert	Messmethode / Bemerkungen
Servicezeit 7x24	7x24h (365 Tage)	• Montag – Sonntag 00:00 – 24:00 Uhr, inkl. nationale Feiertage • keine „planned downtime“, d.h. keine periodischen Wartungsfenster mit Serviceunterbruch, nur geplante und angekündigte Wartungen • Wartungen und Changes mit Serviceunterbruch nur nach gegenseitiger Vereinbarung • Arbeiten mit Serviceunterbruch sind in einem speziellen Verfahren mit Einbezug der Nutzer zu bewilligen (min. 15 Arbeitstage Vorlaufzeit)

Tabelle 10.2 Standard Servicezeit

Die Servicezeit für sämtliche Anlagen und Services der BSA ist immer 7x24h. Es werden keine alternativen Servicezeiten definiert.

10.1.2 Supportzeit

Die **Supportzeit** definiert die Zeitspanne (Tageszeiten, die Wochentage sowie die nationalen Feiertage), während der Unterstützung für den angebotenen Service am Service Access Point garantiert ist. Während der Supportzeit wird bei einem Service Ausfall innerhalb der vertraglich vereinbarten Reaktionszeit ein Trouble-Ticket eröffnet und unmittelbar mit der Wiederherstellung des Service begonnen.

Das Attribut **Reaktionszeit** ist definiert als die Zeitspanne von der Service-Ausfallmeldung (durch Kunde oder durch Überwachungs-Systeme) bis zur ersten Information an den Kunden und der Eröffnung des Trouble Tickets im System.

Messgrösse	Wert	Messmethode / Bemerkungen
Supportzeit 7x24	7x24h (365 Tage)	• Montag – Sonntag 00:00 – 24:00 Uhr, inkl. nationale Feiertage • Reaktionszeit des Service Desk oder der Pikettorganisation bei Störungsmeldungen: max. 15 Minuten nach Ausfallmeldung

Tabelle 10.3 Standard Supportzeit

Die Supportzeit für sämtliche Anlagen und Services der BSA ist immer 7x24h. Es werden keine alternativen Supportzeiten definiert.

10.1.3 Verfügbarkeit

Die **Verfügbarkeit** ist ein Service Level Merkmal eines Service oder eines Service-Elements, welches beschreibt, wie die geforderte und vereinbarte Funktionalität zu einem bestimmten Zeitpunkt oder während einer definierten Periode zu erfüllen ist.

Dabei bedeutet **Downtime**[9] die Summe aller Service Ausfallzeiten in Stunden und Minuten innerhalb der definierten Messperiode, bei der ein Service am entsprechenden Service Access Point während der vereinbarten Supportzeit nicht verfügbar und damit die minimale Funktionalität nicht gewährleistet ist.

Der Service Level Parameter Verfügbarkeit steht in unterschiedlichen Gütestufen zur Auswahl.

Messgrösse	Wert	Messmethode / Bemerkungen
Downtime 2h	≤ 2h pro Jahr	• Nur zu erreichen mittels redundanten Verbindungen • Gemessen pro Jahr und redundantem Anschluss (redundante Service Access Points) • Redundanzverlust d.h. Verlust einer Verbindung muss innert 24h behoben werden • Max. 1 Ausfall pro Jahr zugelassen
Downtime 8h	≤ 8h pro Quartal	• Gemessen pro Quartal und Anschluss (Service Access Point) • Max. 2 Ausfälle pro Quartal zugelassen
Downtime Best Effort	Keine Vorgabe	• Ziel ist es, einen Ausfall innerhalb 24h zu beheben

Tabelle 10.4 Übersicht Verfügbarkeit

10.1.4 Stromautonomie

Die **Stromautonomie** sagt aus, wie lange ein System bei Ausfall der öffentlichen Stromversorgung mittels eigener Notstromversorgung noch funktionieren muss.

Die Stromautonomie auf dem IP-Netz BSA dient dazu, bei einer Strommangellage bzw. einem Stromausfall noch für eine gewisse Zeit, die am IP-Netz BSA angeschlossenen Geräte und Systeme zu erreichen. Für gewisse Anlagen kann es durchaus sein, dass eine höhere Stromautonomie gefordert wird.

Messgrösse	Wert	Messmethode / Bemerkungen
Stromautonomie 1h	> 1h	• Gemessen pro Ereignis
Stromautonomie Best Effort	Keine Vorgabe	• n.a.

Tabelle 10.5 Übersicht Stromautonomie

[9] Ausfälle verursacht durch höhere Gewalt wie bspw. Naturkatastrophen oder ein von aussen kommendes, unvorhersehbares und unbeherrschbares aussergewöhnliches Ereignis, das auch durch äusserste Sorgfalt nicht verhütet bzw. abgewendet werden kann (z.B. schwerer Verkehrsunfall, Sabotage, etc.), geht nicht in die Downtime ein.

10.2 Service Level Zuordnung IP-Netz BSA

Die folgende Tabelle zeigt die Zuordnung der einzelnen Service Levels zu bestimmten Elementen des IP-Netzes BSA.

	Stromautonomie 1h	Stromautonomie Best Effort	Servicezeit 7x24 (365 Tage)	Supportzeit 7x24 (365 Tage)	Downtime 2h (pro Jahr)	Downtime 8h (pro Quartal)	Downtime Best Effort
Backbone Anschluss GE / VMZ-CH / BSA-RZ (redundanter Anschluss über zwei Router)	X	--	X	X	X	--	--
Anschluss Perlenkette IP-Netz BSA GE Abschnitt / ELZ/BLZ (redundanter Anschluss über zwei Router)	X	--	X	X	X	--	--
Access Switch	X	(X)	X	X	--	X	(X)
NTP	X	--	X	X	X	--	--
DMZ GE / VMZ-CH	X	--	X	X	--	X	--
NMS GE / VMZ-CH	X	--	X	X	--	X	--
IPAM/DDI-Tool	X	--	X	X	--	X	--
DHCP / DNS	X	--	X	X	--	X	--

X = Standard (X) = kann in begründeten Ausnahmen angewendet werden

Tabelle 10.6 Service Level Zuordnung für das IP-Netz BSA

10.3 Zentraler und dezentraler Betrieb

Die Elemente des IP-Netzes BSA werden unterschiedlich betrieben.

- Der Betrieb von folgenden Elementen bleibt weiterhin bei den GE bestehen und wird durch die GE geführt:
  - IP-Netz BSA GE;
  - Network Management System (NMS);
  - DNS-Server (konfiguriert durch IPAM/DDI-Tool);
  - DHCP-Server (konfiguriert durch IPAM/DDI-Tool);
  - DMZ/Firewalls/RAS.

Die benötigte Infrastruktur ist jeweils pro GE vorhanden, ebenso besteht pro GE eine entsprechende Betriebsorganisation.

- Zentral betrieben werden folgende Elemente:
  - IPAM/DDI-Tool;
  - E2E-Service Monitoring Tool;
  - Takt- und Zeitsynchronisation (Referenz für ASTRA-Zeit und -Takt);
  - Inventarsysteme.

Die benötigte Infrastruktur wird zentral aufgebaut, aber dezentral genutzt. Die notwendige Betriebsorganisation für den Betrieb und Unterhalt der Systeme ist einmal vorhanden. Die Datenpflege der Nutzerdaten erfolgt in der Verantwortung der Gebietseinheiten.

Die konkreten Umsetzungen sind den jeweiligen ASTRA Dokumentationen zu entnehmen.

11 Steuerung IP-Netz BSA

Die Steuerung des IP-Netzes BSA erfolgt zentral durch das Produktmanagement IP-Netz BSA. Das Produktmanagement übernimmt folgende Aufgaben:

- Das Produktmanagement definiert und verantwortet nach den Vorgaben von SA-CH und in enger Abstimmung mit SA-CH die Gesamtarchitektur IP-Netz BSA inkl. der notwendigen Support Systeme, der Basisdienste und zentralen Tools und passt diese laufend den Bedürfnissen an;
- Das Produktmanagement steht in engem Kontakt mit internen und externen Partnern und Organisationen und klärt deren Bedürfnisse und Anforderungen hinsichtlich Kommunikationsservices BSA ab;
- Es nimmt die Anforderungen an das IP-Netz BSA, an die Basisdienste und zentralen Tools und an die Netzwerk-Security auf und legt in enger Abstimmung mit SA-CH die Richtlinien fest, damit eine homogene, leistungsfähige und hochverfügbare Kommunikationsinfrastruktur zur Verfügung steht;
- Es legt den Grad der Standardisierung des Netzwerkes, der notwendigen Support Systeme und der Services in enger Zusammenarbeit mit dem Betrieb in den Filialen/GE und dem Betrieb der zentralen Support Systeme fest;
- Das Produktmanagement legt nach den Vorgaben von SA-CH und in enger Abstimmung mit SA-CH die Strategie fest, was selber produziert und was als Fremdleistung bezogen wird (Servicebezug). Dies erfolgt in Abstimmung mit den Richtlinien des ASTRA und des Bundes. Es legt die entsprechenden Beschaffungskonzepte fest;
- Das Produktmanagement koordiniert und unterstützt die Filialen bei der Migrationsplanung und der Umsetzung der Richtlinien.

Glossar

Begriff/Abkürzung	terme/abréviation	Bedeutung
(BSA) Abschnitt	section (EES)	logischer Abschnitt für BSA, nicht der Streckenabschnitt
(Netzwerk-)Segment	segment (de réseau)	Segmente gemäss ASTRA 83040 (meist VLAN)
(Netzwerk-)Zone	zone (de réseau)	im Sinne der NSP des Bundes Si003 (getrennt durch PEZ)
(Teil-)Anlage	(partie d')installation	nur im Sinn der AKS-Definitionen gebraucht
Access-Bereich	niveau accès	L2-Struktur, die den Zugang (Userport) den Endgeräten bereitstellt
AKS-CH		Struktur und Kennzeichnung der Betriebs- und Sicherheitsausrüstungen
AR		Abschnittsrechner
AS		Anlagensteuerung
Ausrüstung/Gerät	équipement	jede Art von aktiven Geräten im BSA-Umfeld (auch ohne Verbindung zum IP-Netz BSA)
Backbone/BB	backbone/BB	Vom Bund (L3 durch BIT, Übertragung durch FUB) bereitgestellte nationale Vernetzung aller Teilnetze
BD (Basisdienste)	BD (services de base)	Netzwerk-Basisdienste (IPAM-Tool, DNS, Zeitquellen, …) für das gesamte IP-Netz BSA
Betriebsleitebene		Diese Ebene bietet die Überwachung und Bedienung aller Anlagen einer Strecke mittels Betriebsleitrechnern, einerseits durch die Polizei hinsichtlich Ereignissen und speziellen betrieblichen Aspekten, andererseits durch den Unterhaltsdienst hinsichtlich Funktionsbereitschaft der Anlagen. Die Betriebsleitrechner sind über ein Kommunikationsnetzwerk mit den Abschnittsrechnern verbunden. Andere Bezeichnung: Übergeordnete Leitebene
BGP (iBGP/eBGP)	BGP	Ein IP-Routing-Protokoll mit vielfältigen Funktionen zum Austausch komplexer Topologieinformationen. Wird iBGP als netzwerk-internes Protokoll und als eBGP am externen Übergang zu Fremdnetzen eingesetzt (aus dem Englischen: Border Gateway Protocol).
BLZ	BLZ	Betriebsleitzentrale
BSA	EES	Betriebs- und Sicherheitsausrüstungen
BSA-Abschnitt	section EES	Von einem Abschnittsrechner gesteuerter Abschnitt der Nationalstrasse
BSA-Region	région EES	Anlagenspezifisch definierte Region, in der es eine regional übergeordnete Steuerung gibt
Client/Host Server	client/hôte serveur	allgemeine ICT-Begriffe (keine BSA-spezifische Bedeutung), Verwendung bei der Beschreibung von Protokollen
DAB	DAB	Digital Audio Broadcasting
DDI	DDI	DNS, DHCP and IP Address Management
DHCP	DHCP	Das Dynamic Host Configuration Protocol (DHCP) ist ein Kommunikationsprotokoll in der Computertechnik. Es ermöglicht die Zuweisung der Netzwerkkonfiguration an Clients durch einen Server. DHCP wurde im RFC 2131 definiert und bekam von der Internet Assigned Numbers Authority die UDP-Ports 67 und 68 zugewiesen.
Dienst	service	Dienst ist ein Obergriff sowohl für Fachdienste wie auch für Basisdienste. Dienste implementieren Zugriffs- und Verarbeitungslogik, verfügen aber nicht über eine Benutzeroberfläche.
DMZ	DMZ	Vorgelagerte Sicherheitszone, die von aussen den Zugriff unter weniger hohen Auflagen zulässt, als die nachgelagerten inneren Zonen mit höherem Schutzbedarf (aus dem Englischen für Demilitarized Zone)

Begriff/Abkürzung	terme/abréviation	Bedeutung
DNS	DNS	Das Domain Name System (DNS) ist einer der wichtigsten Dienste in vielen IP-basierten Netzwerken. Seine Hauptaufgabe ist die Beantwortung von Anfragen zur Namensauflösung. Das DNS funktioniert ähnlich wie eine Telefonauskunft.
Domäne	domaine	Die Domäne ist ein Bereich um Dinge zu ordnen oder zusammen zu fassen. Beim ASTRA wird die Domäne verwendet für: Namensraum: Innerhalb eines Namensraums sind Identitäten eindeutig, d.h. es gibt nicht mehrere Identitäten für die gleiche Ressource. Funktionsdomäne: Zusammenfassung verschiedener Funktionen. Fachdomäne: Zusammenfassung verschiedener Fachdienste. Prozessdomäne: Zusammenfassung verschiedener Prozesse.
ELZ	ELZ	Einsatzleitzentrale (der Polizei).
Endgerät	équipement terminal	jede Art von Ausrüstung an einem Userport des IP-Netzes BSA
ERPS	ERPS	Ethernet Ring Protection Switching, oder ERPS, ist ein Standard-Protokoll gemäss ITU-T G.8032 auf dem Layer-2, um deterministische Redundanz-Umschaltzeiten von unter 50ms in komplexen Ringstrukturen zu garantieren.
Erschliessungsring	anneau de raccordement	MPLS-Struktur, die alle BSA-Abschnitte einer GE verbindet
F/Filiale	F/filiale	Filiale (fünf regionale Einheiten des ASTRA)
Firewall	firewall/pare-feu	Eine Firewall ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt.
GE	UT	Gebietseinheit (11 überkantonale organisatorischen Einheiten, die ihr eigenes IP-Netz BSA GE betreiben)
GUI	GUI	Graphical User Interface (Benutzeroberfläche)
IEC	IEC/CEI	Die Internationale Elektrotechnische Kommission ist eine internationale Normungsorganisation im Bereich der Elektrotechnik und Elektronik. Für viele Industrieanwendungen bezieht sie auch Netzwerktechnogien ein.
IEEE	IEEE	Das Institute of Electrical and Electronics Engineers ist ein weltweiter Berufsverband, der unter anderem Gremien für die Standardisierung von Techniken, Hardware und Software bildet. Speziell im Bereich der Ethernet-Technologie ist das IEEE massgebend.
IETF	IETF	Die Internet Engineering Task Force (IETF, englisch für ‚Internettechnik-Arbeitsgruppe') ist eine Organisation, die sich mit der technischen Weiterentwicklung des Internets. Sie ist der de-facto Standardisierungskörper im gesamten IP-Umfeld.
IP	IP	Internet Protokoll
IPAM	IPAM	IP Address Management
IP-Netz BSA GE GE Abschnitt BD VMZ Backbone	réseau IP EES UT UT section BD VMZ Backbone	Ein IP-Netz für die Betriebs- und Sicherheitsausrüstung der Nationalstrassen mit fol-genden Elementen (Teilnetzen): - 11 IP-Netze BSA GE - dem IP-Netz BSA Backbone (Backbone der Bundesverwaltung) - Verbindungen zur VMZ-CH - Verbindungen zu den Rechenzentren BSA - Verbindungen zu den BD (Basisdiensten des IP-Netz BSA)
ITU-T	ITU-T	Die Internationale Fernmeldeunion (englisch International Telecommunication Union, ITU) ist eine Sonderorganisation der Vereinten Nationen und die einzige Organisation, die sich offiziell und weltweit mit technischen Aspekten der Telekommunikation beschäftigt.
LDP	LDP	Ein MPLS-Protokoll zur netzwerkweiten Verwaltung der logischen LSP-Pfade und deren Bezeichnung (den MPLS-Label). Aus dem Englischen von Label Distribution Protocol.

Begriff/Abkürzung	terme/abréviation	Bedeutung
Leitebene	niveau gestion	Siehe Prozessleitebene
Leitsystem	système de gestion	Dient dem Bedienpersonal zur Überwachung und Leitung von Anlagen
Leittechnik	système de commande/gestion	Funktionen und Komponenten, die der Überwachung und Leitung von Anlagen dienen.
LS	LS	Lokalsteuerung
LWL	LWL	Lichtwellenleiter
Management-Ebene (auch Mgmt-Ebene oder ME)	niveau management (ou ME)	zentrale, übergeordnete Leitebene
Monitoring	monitoring	Überwachung und Visualisierung der technischen Funktionen der Anlagen und Leitsysteme.
MPLS	MPLS	Multiprotocol Label Switching (MPLS) ermöglicht die Übertragung von Datenpaketen in entlang eines zuvor aufgebauten Pfads zur Bildung virtueller L2 und L3 Netze.
NAC	NAC	Network Access Control
Netzwerkausrüstung	équipement réseau	alles (inkl. Firewall, Management-Systeme, …)
Netzwerkelement	élément réseau	nur aktive Übertragungsausrüstung (Router oder Switch)
NMS	NMS	Network Management System
NNI (Erschliessungsring)	NNI (anneau de raccordement)	Die Netzwerk-Netzwerk-Interfaces (NNI) sind die Schnittstellen der Netzwerkelemente im Erschliessungsring zueinander. Im Gegensatz zum Userport werden an den NNI keine Endgeräte angeschlossen.
OT	OT	Operational Technology
Prozessleitebene	niveau processus	Begriff aus der Leittechnik: In dieser Ebene erfolgen die Überwachung und Bedienung aller Anlagesteuerungen und die übergeordnete Steuerung (Tunnelreflexe) innerhalb eines Abschnitts mittels eines Abschnittsrechners.
QoS	QoS	Quality of Service (QoS) oder Dienstgüte beschreibt die Güte eines Kommunikationsdienstes aus der Sicht der Anwender, das heisst, wie stark die Güte des Dienstes mit deren Anforderungen übereinstimmt.
RFC	RFC	Die RFC (Requests for Comments) beinhalten technische und organisatorische Dokumente über das Internet. Einige RFC, jedoch nicht alle, stellen Internetstandards dar und müssen hohe Anforderungen erfüllen und einen Gemeinschaftskonsens der Internet Engineering Task Force (IETF) darstellen.
Router	routeur	gemeint sind immer die Router der Erschliessungsringe (IP/MPLS oder SegementRouting), sonst explizit benannt (z.B. Spoke-Site-Router).
Router	routeur	Router oder Netzwerkrouter sind Netzwerkgeräte, die Netzwerkpakete zwischen mehreren Rechnernetzen weiterleiten können.
RSVP	RSVP	Eigentlich RSVP-TE (Englisch für Resource Reservation Protocol - Traffic Engineering) ist beim IP-Netz BSA ein Protokoll zum Aufbau der logischen Pfade bei MPLS.
rVDE	rVDE	Regionale Verkehrsdatenerfassung
rVL	rVL	Regionale Verkehrslenkung
RZ(-BSA)	RZ(-EES)	Rechenzentrum BSA
SAP	SAP	Service Access Point: Im IP-Netz BSA ist dies i.d.R. ein physisches Port eines Switches oder Routers.
SCADA-System	système SCADA	SCADA-Systeme (Supervisory Control and Data Acquisition) oder auch ICS- bzw. DCS-Systeme (Industrial Control Systems bzw. Distributed Control Systems) sind vernetzte Computer-Systeme (Leitsysteme) für die Überwachung, Steuerung und Optimierung von Industrie-Anlagen.

Begriff/Abkürzung	terme/abréviation	Bedeutung
Segment Routing/SR	Segment Routing/SR	SR ist ein mögliche Nachfolgetechnologie für MPLS und ermöglicht die Übertragung von Datenpaketen in entlang eines zuvor aufgebauten Pfads zur Bildung virtueller L2 und L3 Netze.
Service	service	Siehe Dienst
SLA	SLA	Service Level Agreement
SPB	SPB	EthShorted Path Bridging, oder SPB, ist ein Standard-Protokoll gemäss IEEE 802.1aq auf dem Layer-2, um deterministische Redundanz-Umschaltzeiten von in beliebigen Topologien zu garantieren und die Ressourcen optimal zu nutzen..
Switch	commutateur	gemeint sind immer die L2-Netzwerkelemente des Access-Layers, sonst entsprechend bennantbenannt.
Systemarchitektur	architecture du système	Ein Modell eines Systems, das den Zusammenhang und die Eigenschaften der verschiedenen Elemente und ihrer Funktionen beschreibt.
UeLS	UeLS	Übergeordnetes Leitsystem
ULA	ULA	Unique Local Address
UNI (Erschliessungsring)	UNI (anneau de raccordement)	Die User-Netzwerk-Interfaces (UNI) sind die Schnittstellen der Netzwerkelemente im Erschliessungsring zu den Switchen des Access-Layers.
Uplink (Access-Layer)	uplink (niveau accès)	Die Ethernet-Schnittstelle des Access-Layers zur Verbindung an das UNI des Routers im Erschliessungsring.
Userport (Access-Layer)	userport (niveau accès)	Die physische Ethernet-Schnittstelle am Access-Layer für den Anschluss der Endgeräte am IP-Netzes BSA.
VM-CH	gestion du trafic en Suisse	Verkehrsmanagement Schweiz
VMZ(-CH)	VMZ(-CH)	Verkehrsmanagementzentrale Schweiz
WDM	WDM	Mehrfachnutzung (Multiplex) einer LWL mit verschiedenen optischen Wellenlängen (engl. Wavelength Division Multiplex)

Literaturverzeichnis

Richtlinien und Dokumentation des ASTRA

[1]	Bundesamt für Strassen ASTRA, „**Struktur und Kennzeichnung der Betriebs- und Sicherheitsausrüstung (AKS-CH)“,** *Richtlinie ASTRA 13013*, www.astra.admin.ch
[2]	Bundesamt für Strassen ASTRA, „**Sicherheit Leit- und Steuersysteme der Betriebs- und Sicherheitsausrüstung**“, *Richtlinie ASTRA 13030,* www.astra.admin.ch
[3]	Bundesamt für Strassen ASTRA, „**IP-Adressierung für BSA“**, *Dokumentation 83040*, www.astra.admin.ch
[4]	Bundesamt für Strassen ASTRA, „**Aufbau und den Betrieb des IPAM/DDI-Tools für BSA“**, *Dokumentation 83041*, (noch nicht publiziert)
[5]	Bundesamt für Strassen ASTRA, „**Network Security Policy (NSP) IP-Netz BSA“**, *Dokumentation 83042*, (noch nicht publiziert)
[6]	Bundesamt für Strassen ASTRA, „**Kabelanlagen der Nationalstrassen“**, *Richtlinie ASTRA 13022,* www.astra.admin.ch
[7]	Bundesamt für Strassen ASTRA, „**IP-Netz BSA Zeit- und Taktverteilung “**, *Dokumentation 83044,* www.astra.admin.ch
[8]	Bundesamt für Strassen ASTRA, „**Betriebs- und Sicherheitsausrüstung (FHB BSA)“**, *Fachhandbuch 23001*
[9]	Bundesamt für Strassen ASTRA, **„IP-Netz BSA - Verbindung der Streckensysteme“,** *Dokumentation 83045,* www.astra.admin.ch

Auflistung der Änderungen

Ausgabe	Version	Datum	Änderungen
2017	1.30	10.08.2022	Diese Revision enthält neben vielen kleineren Anpassungen und Präzisierungen vor allem folgende Punkte: • Alle Kap.: Texte und Abbildungen mit dem IP-Netz BSA BD bzw. den Basisdiensten erweitert • Kap. 2.3: Verweis angepasst Ref. 6 • Kap. 2.5: Architektur der Erschliessungsringe präzisiert, Standard-designs eingefügt • Kap. 2.6 präzisiert • Kap. 3: Netzwerkprotokolle um Segment Routing und ERPS erweitert, Kapitel generell präzisiert • Kap. 3.8 mit Dokumentation 83044 abgeglichen • Kap. 4 ergänzt • Kap. 5 mit Dokumentation 83040 abgeglichen • Kap. 7 und 8 an Neufassung der Richtlinie 13030 angeglichen • Kap. 10.1.3: Downtime angepasst • Kap.11 an Strategie Produktmanagement angepasst
2017	1.20	15.04.2019	Formelle Anpassungen der französischen Version: das Wort «section» ersetzt «tronçon».
2017	1.10	15.12.2018	Präzisierungen in den Kapiteln 1.2 Geltungsbereich, 2.5 Erschliessungsringe, 2.6 Access im lokalen Abschnitt, 5.2 und 5.3 IP-Adressierung und Ergänzungen im Glossar. Publikation der französischen Version.
2017	1.00	07.12.2017	Inkrafttreten Ausgabe 2017.