



Daniel Gähwiler / Patrick Gerber, 31. Oktober 2019

# IP-Netz BSA – FAQ

## Impressum

Erstelldatum / Revisionsdatum:	31.10.2019
Ersteller/in:	Daniel Gähwiler / Patrick Gerber, CSI Consulting AG
Verzeichnis / Dateiname:	2019-10-31_D_IPNetzBSA_FAQ_V1.3.docx
Anzahl Seiten:	
Genehmigt am:	31.10.2019
Genehmigt von:	Jean-Paul Schnetz

## Änderungsverzeichnis

Version	Datum	Ersteller	Bemerkungen
0.1	06.06.19	Ga	Erstversion
0.7	25.06.19	Ga	Alle Kapitel ergänzt
0.9	03.07.19	Ge/Ga	Alle Kapitel ergänzt
1.0	08.07.19	Ga	Nach Review mit Scj
1.1	06.09.19	Ga/Ge	Neue oder überarbeitete Kapitel gelb hinterlegt
1.2	10.10.19	Ge/Ga	Neue oder überarbeitete Kapitel gelb hinterlegt (im Vergleich zu V1.1), Änderungsverzeichnis am Schluss des Dokuments
1.3	31.10.19	Ga/Ge	Änderungsverzeichnis am Schluss des Dokuments



## INHALTSVERZEICHNIS

IP-Netz BSA – FAQ	1
1. Begriffe	5
1.1. Was wird unter dem Begriff BSA-Abschnitt verstanden?	5
2. Access im lokalen IP-Netz BSA GE Abschnitt	6
2.1. Gibt es Umsetzungsbeispiele zur Referenzarchitektur?	6
2.2. Dürfen Access-Switches über den BSA-Abschnitt hinweg an MPLS-Routern erschlossen werden?	6
2.3. Dürfen Access-Switches Perlenketten über zwei BSA-Abschnitte bilden?	6
2.4. Dürfen Ketten von Access-Switches am Anfang und Ende an zwei verschiedenen MPLS-Routern im selben Raum terminieren?	6
2.5. Wie viele Perlenketten von Access Switches dürfen pro MPLS-Router angeschlossen sein?	6
2.6. Müssen Access Switches immer in Ketten (Kaskaden) angeschlossen sein?	6
2.7. Dürfen gestackte Access-Switches eingesetzt werden?	6
2.8. Dürfen Access-Switches mit L3/Routing eingesetzt werden?	6
2.9. Müssen Access-Switches mit 10-Gigabit-Schnittstelle verwendet werden?	6
2.10. Weshalb kommt kein MPLS in den Access-Layer?	7
2.11. Welche L2-Konfiguration empfehlen Sie für den Access-Layer?	7
3. Erschliessungsringe	8
3.1. Muss jeder BSA-Abschnitt zwei MPLS-Router haben?	8
3.2. Darf ein BSA-Abschnitt ohne MPLS-Router realisiert werden?	8
3.3. Dürfen die Erschliessungsringe auch als vermaschte Strukturen gebaut werden?	8
3.4. Sind direkte Verbindungen zwischen Erschliessungsringe verschiedener GE möglich?	8
3.5. Gehört der MPLS-Router zu einem BSA-Abschnitt?	8
4. Netzkomponenten	9
4.1. Gibt es Musterbeispiele technische Spezifikationen Netzausrüstung?	9
4.2. Wie ist die 100 Gbit-Technologie einzusetzen? Was ist darunter zu verstehen?	9
4.3. Gibt es Produktempfehlungen zu den MPLS-Routern?	9
4.4. Inwieweit müssen die Vorgaben der RiLi umgesetzt werden?	9
4.5. Muss man mit managed Switches bis auf die Feldebene gehen?	9
4.6. Werden im Access-Bereich unterschiedliche Switches eingesetzt?	9
4.7. Muss die Ausrüstung IP-Netz BSA in einem separaten Schrank untergebracht werden?	9
4.8. Müssen Netzwerkelemente, welche End of Support sind, ersetzt werden?	10
4.9. Wie wird die Zeit- und Taktverteilung aufgebaut?	10
5. IP-Netz BSA Backbone	11
5.1. Sind die Übergabepunkte von den IP-Netz BSA GE zum Backbone IP-Netz BSA festgelegt?	11
5.2. Ab wann steht der Backbone IP-Netz BSA zur Verfügung?	11
5.3. Was müssen die Filialen/GE für den Backbone IP-Netz BSA zur Verfügung stellen?	11
5.4. Wie ist der Übergang zum Backbone technisch realisiert bzw. welche technischen Anforderungen müssen die Router ASTRA-seitig erfüllen?	11
5.5. Werden die Verbindungen zum Bundesverwaltungsnetz (BV-Netz, Office Netz) bestehen bleiben?	11
6. IP-Adressierung	12
6.1. Welche Geräte sollen in einem ersten Schritt auf IPv6 migriert werden?	12
6.2. Dürfen die einzelnen Anlagen in den Abschnitten noch mit IPv4 adressiert werden?	12
7. DNS, DHCP und IP Address Management (IPAM/DDI)	12

7.1.	Wann wird das IPAM-Tool für die GE zur Verfügung stehen?	12
7.2.	Unterstützt das IPAM-Tool auch die Verwaltung von IPv4?	12
7.3.	Welche Systeme muss die GE im Bereich IP-Adressvergabe und Namensauflösung aufbauen?	12
8.	Security und Netzwerkzonen	13
8.1.	Werden die Vorgaben Bund in den Sicherheitsrichtlinien ASTRA berücksichtigt?	13
8.2.	Sind künftig lokale Übergänge verboten?	13
8.3.	Werden im IP-Netz BSA der GE Firewalls zum Backbone IP-Netz BSA eingesetzt?	13
8.4.	Was muss mit den Netzübergängen zu Fremdnetzen und dem Internet angepasst werden?	13
9.	Network Access Control	13
9.1.	Ab wann wird das NAC-Tool zur Verfügung stehen?	13
9.2.	Wird das NAC-Tool ebenfalls zentral zur Verfügung gestellt?	13
10.	Network Management System	14
10.1.	Wird das NMS auch zentral für den Betrieb in den GE zur Verfügung gestellt?	14
11.	Betrieb	14
11.1.	Werden Service Levels einheitlich definiert und vorgegeben?	14
11.2.	Werden die Betriebsprozesse für das IP-Netz BSA vorgeschrieben?	14
12.	Änderungsverzeichnis	15
12.1.	Neu in FAQ V1.3	15
12.2.	Neu in FAQ V1.2	15
12.3.	Neu in FAQ V1.1	15

# 1. Begriffe

## 1.1. Was wird unter dem Begriff BSA-Abschnitt verstanden?

Der Begriff BSA-Abschnitt ist gemäss ASTRA Richtlinie 13031, Kap. 2.4.3 wie folgt definiert:

«Ein BSA-Abschnitt ist ein Stück der Nationalstrasse, das funktional eine abgeschlossene Einheit für die Betriebs- und Sicherheitsausrüstung bildet. Der Abschnittsrechner übernimmt die Überwachung und übergeordnete Steuerung im BSA-Abschnitt sowie die Anbindung an die Management-Ebene. Der BSA-Abschnitt ist nicht zwingend identisch mit dem UPlaNS-Abschnitt. Der BSA-Abschnitt ist für alle Anlagen identisch (siehe auch Richtlinie 13031, Abb. 2.3).

Für mögliche Abweichungen (z.B. Signalisation) siehe Richtlinie 13031, Kapitel 5.3. Der Perimeter einer Signalisationsanlage kann mehr als einen BSA-Abschnitt umfassen.

Bei der Bildung von Abschnitten sind die folgenden Regeln umzusetzen:

- BSA-Abschnitte werden nur dort definiert, wo BSA vorhanden sind (Siehe Richtlinie 13031, Kapitel 5.3.2).
- Sie verfügen immer über einen Abschnittsrechner.
- Ein Tunnel, der gemäss dem Prozess in Richtlinie 13031, Kapitel 5.3.2 mit einem eigenen Abschnittsrechner ausgerüstet wird, bildet einen eigenen BSA-Abschnitt (inkl. Vorzonen und eventuell vorhandener offener Strecke).
- Ein Tunnel, der nicht mit einem eigenen Abschnittsrechner ausgerüstet wird, wird einem BSA-Abschnitt zugeteilt und von dem dortigen Abschnittsrechner gesteuert. Dies kann auch der Abschnittsrechner eines anderen Tunnels sein (Überlappung von Anlagen).
- Eine offene Strecke mit BSA (z.B. Pannestreifenumnutzung) kann ebenfalls einen BSA-Abschnitt bilden.
- Die BSA-Abschnittslänge richtet sich nach der Ausdehnung von lokal zusammengehörigen BSA.
- Einzelne abgelegene Aktoren oder Sensoren (insbesondere z.B. Signale) gehen nicht in die Bestimmung der Ausdehnung des BSA-Abschnitts ein. Solche Aktoren / Sensoren sind wie alle anderen mit den Steuerungen des Abschnitts verbunden, liegen aber auf dem Perimeter eines Nachbarabschnitts.
- Ein BSA-Abschnitt kann in Teilabschnitte unterteilt werden. Dies ist insbesondere bei Tunnelobjekten sinnvoll. Bei Anlagen mit Lokalsteuerungen werden alle Aggregate eines Teilabschnitts von jeweils einer LS gesteuert.
- Diese Teilabschnitte orientieren sich an den Energiegrenzen. Ausschaltungen und Ausfälle in der Niederspannungsversorgung sollen einen Teilabschnitt immer entweder vollständig, oder gar nicht betreffen.»

## **2. Access im lokalen IP-Netz BSA GE Abschnitt**

### **2.1. Gibt es Umsetzungsbeispiele zur Referenzarchitektur?**

Ja, siehe Dokument «2019-09-06\_IPNetzBSA\_Beispielzeichnungen\_Zielarchitektur\_V1.1.vsd».

### **2.2. Dürfen Access-Switches über den BSA-Abschnitt hinweg an MPLS-Routern erschlossen werden?**

Ja, sie dürfen. Im Sinne der Wegredundanz ist empfohlen, dem Streckenverlauf zu folgen und die Zweitabschliessung im nächsten Abschnitt vorzunehmen. (Siehe Dokument «2019-07-03\_D\_IPNetzBSA\_Beispielzeichnungen\_Zielarchitektur» Punkt G).

### **2.3. Dürfen Access-Switches Perlenketten über zwei BSA-Abschnitte bilden?**

Nein. Eine Perlenkette von Access-Switches gehört vollumfänglich zu einem dedizierten BSA-Abschnitt. Auch wenn die Perlenkette auf zwei MPLS-Routern in unterschiedlichen BSA-Abschnitten terminiert, bleibt die Kette und sämtliche damit erschlossene BSA-Ausrüstung einem Abschnitt zugeordnet.

### **2.4. Dürfen Ketten von Access-Switches am Anfang und Ende an zwei verschiedenen MPLS-Routern im selben Raum terminieren?**

Nein, dürfen sie nicht. Die Erschliessung muss im Sinne der Wegredundanz an Routern in unterschiedlichen Räumlichkeiten erfolgen.

### **2.5. Wie viele Perlenketten von Access Switches dürfen pro MPLS-Router angeschlossen sein?**

Die RiLi schreibt keine maximal angeschlossene Anzahl Perlenketten pro Router vor. Die Anzahl Ketten ist nur durch die Kapazität der Router begrenzt. Allerdings darf eine Kette von Switches aus maximal sieben Switches zwischen zwei Routern bestehen aufgrund von Laufzeiteinschränkungen und Ausfallbeschränkung.

### **2.6. Müssen Access Switches immer in Ketten (Kaskaden) angeschlossen sein?**

Nein, eine zulässige Abweichung ist die sternförmige Anschliessung von einzelnen Switches («Dual Homing»). (Siehe Dokument «2019-07-03\_IPNetzBSA\_Beispielzeichnungen\_Zielarchitektur» Punkt F). Jeder Access-Switch ist entweder selbst oder über die Kette mit zwei MPLS-Routern verbunden.

### **2.7. Dürfen gestackte Access-Switches eingesetzt werden?**

Nein, aus Sicht Redundanz machen gestackte Switches bei einer Georedundanz keinen Sinn und werden durch die Richtlinie nicht gefordert. Falls aus Kapazitätsgründen gestackte Switches eingesetzt werden, ist dies natürlich sinnvoll.

### **2.8. Dürfen Access-Switches mit L3/Routing eingesetzt werden?**

Nein. Das Routing ist vollumfänglich in den MPLS-Routern umgesetzt. Der Access-Layer ist auf L2 beschränkt.

### **2.9. Müssen Access-Switches mit 10-Gigabit-Schnittstelle verwendet werden?**

Nein. Bei Legacy-Ausrüstung und neuer gehärteter Industriearüstung (Feldebene) ist die Verwendung einer 1 Gigabit-Anbindung an die MPLS-Router in der Regel ausreichend.

## **2.10. Weshalb kommt kein MPLS in den Access-Layer?**

Aus Kostengründen verzichtet die RiLi den MPLS-Layer bis zum Port auf dem Access-Layer auszu-dehnen.

## **2.11. Welche L2-Konfiguration empfehlen Sie für den Access-Layer?**

Zwei Konfigurationen stehen im Vordergrund:

1. Ein VLAN pro Port auf der Access-Kette. Auf dem MPLS-Router wird für jeden Port der Kette der benötigte Dienst konfiguriert. Der Verkehr zwischen den Access-Ports wird von den MPLS-Routern kontrolliert.
2. Lokale VLAN pro logische BSA-Struktur. Ports der gleichen logischen Struktur (z.B. alle Videokameras) sind auf dem Access-Layer ein VLAN und werden als solches dem MPLS-Router übergeben. D.h. L2-Verkehr innerhalb der logischen Strukturen wird im Access-Layer vermittelt, L3 Verkehr zwischen den logischen Strukturen wird von den MPLS-Routern kontrolliert.

### **3. Erschliessungsringe**

#### **3.1. Muss jeder BSA-Abschnitt zwei MPLS-Router haben?**

Nein. Der Access-Layer muss zwar an zwei räumlich getrennten MPLS-Router terminieren, aber diese dürfen in den Nachbarabschnitten liegen.

#### **3.2. Darf ein BSA-Abschnitt ohne MPLS-Router realisiert werden?**

Ja. Die Ketten vom Access-Layer dürfen beidseitig in einem Nachbar-Abschnitt angeschlossen werden, wenn der Abschnitt ohne lokalen MPLS-Router gebaut wird.

Aus betrieblicher Sicht ist aber zu überlegen, ob es sinnvoll ist, Abschnitte ohne eigene MPLS-Router zu implementieren.

#### **3.3. Dürfen die Erschliessungsringe auch als vermaschte Strukturen gebaut werden?**

Ja. Die Grundforderung ist nur, dass jeder MPLS-Router mit mindestens zwei anderen verbunden ist, was zu einer Ringstruktur führt. Jede unabhängige zusätzliche Verbindung erhöht die Redundanz und ist erlaubt.

#### **3.4. Sind direkte Verbindungen zwischen Erschliessungsringe verschiedener GE möglich?**

Nein. Das IP-Netz BSA jeder GE ist in sich geschlossen und hat über das IP-Netz BSA Backbone einen definierten und standardisierten Übergang zu allen anderen GE.

#### **3.5. Gehört der MPLS-Router zu einem BSA-Abschnitt?**

Ja. Das Netzwerkelement selbst gehört zu dem BSA-Abschnitt, in dem es verbaut wurde. Richtig ist, dass die Schnittstellen zum Access-Layer für weitere Abschnitte konfiguriert werden, um die Ketten aus den Nachbarabschnitten zu terminieren. Zum Access-Layer hin kennen die MPLS-Router alle benötigten L2- und L3-Netze (VPLS und VPRN) der Nachbarabschnitte mitsamt den benötigten Redundanzmechanismen (z.B. SPB und VRRP).

## **4. Netzkomponenten**

### **4.1. Gibt es Musterbeispiele technische Spezifikationen Netzausrüstung?**

Ja, es ist ein Dokument mit den technischen Spezifikationen für MPLS-Router, Access-Switches, NMS und Dienstleistungen verfügbar. Die Spezifikationen können als Textbausteine für Ausschreibungen verwendet werden.

### **4.2. Wie ist die 100 Gbit-Technologie einzusetzen? Was ist darunter zu verstehen?**

Technologisch soll 100 Gbit-Technologie eingesetzt werden. D.h. Chassis mit Backplane und Controllerkarte sollen vollumfänglich mit 100 Gbit/s umgehen können. Die eingesetzten Netzwerkkarten sollen aber auf die notwendige Bandbreite ausgelegt werden, wobei in den MPLS-Erschliessungsringen immer mind. 10 Gbit/s zur Verfügung stehen muss.

### **4.3. Gibt es Produktempfehlungen zu den MPLS- Routern?**

Bei allen Netzwerkausrüstern sehen wir geeignete Geräte. Preislich wichtig ist, dass nicht zu alte oder zu funktionsreiche Familien gewählt werden. So ist z.B. bei Nokia die SR 7750 Familie weniger geeignet, als die neuesten 7250 IXR. Bei Cisco stehen ebenfalls die jüngsten Vertreter der ASR Familie im Vordergrund (z.B. 9901). Bei Juniper die ACX5048/5548 oder MX204, bei Huawei die NE20E-S (z.B. S4).

### **4.4. Inwieweit müssen die Vorgaben der RiLi umgesetzt werden?**

Die Richtlinie 13040 muss spätestens mit der nächsten kompletten Erneuerung oder bei einer Teilerneuerung des IP-Netzes BSA umgesetzt werden. Es müssen aber gewisse Bereiche wie Anbindung Backbone IP-Netz BSA, der Einsatz eines IPAM-Tools, die Umsetzung der Sicherheitsrichtlinie oder betriebliche Aspekte bereits früher auf die Anforderungen der Richtlinie umgestellt werden (siehe dazu auch Migrationskonzept IP-Netz BSA vom 23.03.2018). Ziel ist es, in Abstimmung mit dem Lifecycle der Netzwerke, so schnell als möglich Konformität zur Richtlinie zu erreichen.

In der Migrationsplanung, die bis Ende 2019 erstellt werden muss, werden die entsprechenden Massnahmen definiert und das grobe Vorgehen (Konformitätsschritte) aufgezeigt.

### **4.5. Muss man mit managed Switches bis auf die Feldebene gehen?**

Ja, sobald die Feldswitche Teil des IP-Netzes BSA sind, müssen sie aktiv überwacht werden.

Ziel ist es, von lokalen anlagenspezifischen Netzen wegzukommen und ein gemeinsames IP-Netz zu nutzen.

### **4.6. Werden im Access-Bereich unterschiedliche Switches eingesetzt?**

Ja, grundsätzlich werden unterschiedliche Switch-Familien für die Switches in der Feldebene und die Switches in den Tunnelzentralen oder technischen Räumen eingesetzt. Siehe dazu auch die technischen Spezifikationen «2019-09-05\_IPNetzBSA\_SpecsNetzausrüstung\_V1.1».

### **4.7. Muss die Ausrüstung IP-Netz BSA in einem separaten Schrank untergebracht werden?**

Ja, grundsätzlich muss die Ausrüstung der Erschliessungsringe und die Access-Switches in Tunnelzentralen oder in technischen Räumen von Werkhöfen in separaten, eigenen Schränken untergebracht werden. Eine Vermischung von Kommunikationsinfrastruktur und Abschnittsrechnern oder Lokalsteuerungen soll vermieden werden.

Firewalls oder DNS- und DHCP-Server können im Schrank IP-Netz BSA GE untergebracht werden, da diese im weiteren Sinne zur Kommunikationsinfrastruktur gezählt werden können.

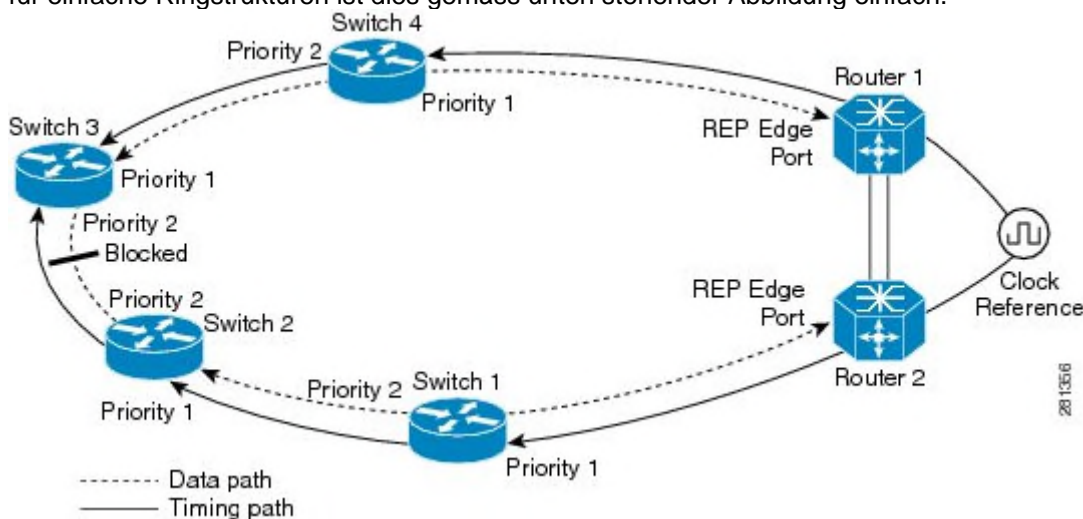
Die Access-Switches der Feldebene bspw. in Tunnelnischen können zusammen mit anderer BSA-Ausrüstung eingebaut werden und müssen nicht strikt getrennt werden.

#### 4.8. Müssen Netzwerkelemente, welche End of Support sind, ersetzt werden?

Ja, Netzwerkausrüstung, welche «end of support» ist oder gehen wird, muss entsprechend ersetzt werden. Dies gilt nicht für Netzwerkausrüstung, welche «end of sale» ist, da in diesen Fällen i.d.R. vom Hersteller noch einige Jahre Support angeboten wird. Allerdings ist zu festzulegen, wie beim Ausfall eines nicht verfügbaren Gerätes der Ersatz abläuft.

#### 4.9. Wie wird die Zeit- und Taktverteilung aufgebaut?

Jede GE verfügt über eine präzise Zeit- und Taktverteilung in den Erschliessungsringen über die Kombination von SyncE (G.8261/G.8262/G.8264) und PTP (IEEE 1588-2008 über IPv6). Während die Konfiguration von PTP eine einfache Konfiguration (vergleichbar komplex wie NTP), muss für SyncE jede GE ein Design erarbeiten, das für jedes NE (in den Erschliessungsringen) zwei Quellen vorsieht. für einfache Ringstrukturen ist dies gemäss unten stehender Abbildung einfach.



Bei realen Netzen mit vermaschten NE, Sticherschliessungen oder anderen Eigenheiten, erfordert das Aufsetzen aller redundanten Synchronisationspfade eine sorgfältige Planung. Zeit- und Taktquellen stehen sowohl zentral über den Backbone IP-Netz BSA bereit als auch durch die GE aufgebaut sein. Die Dokumentation «83044 IP-Netz BSA: Zeit- und Taktverteilung» ist aktuell in Bearbeitung und wird im November 2019 in einer Entwurfsversion vorliegen.

Im Hinblick auf die Migrationsplanung kann aber bereits Folgendes gesagt werden: Zwei redundante Quellen stellt das ASTRA zentral bereit. Über den Backbone IP-Netz BSA werden sowohl die Zeit (über PTP) wie auch der Takt (via SyncE) den GE übergeben. Die Stabilität der zentralen Zeit- und Taktquellen entspricht einem Rubidium-Normal. Die GE können über die redundanten Zugänge zum Backbone diese Signale in den Erschliessungsringen weiterverteilen und ihre MPLS-Router als lokale Quelle einrichten. Alternativ kann eine GE ihre eigenen Zeitquellen (typischerweise eine Rubidium-Uhr mit Satelliten-Zeitreferenz) betreiben. Diese können autark oder im Verbund im den zentralen Quellen aus dem Backbone betrieben werden.

Die Zeit (PTP und NTP) und der Takt (SyncE) werden im Erschliessungsring auf alle MPLS-Router verteilt, die im BSA-Abschnitt als lokaler Zeitserver auftreten. Eine Verteilung des Taktes im Access-Bereich ist nicht vorgesehen. Für die Anspeisung der Endgeräte lassen sich aus PTP die heute üblichen PPS und IRIG gewinnen.

Die Mehrzahl der Endgeräte wird initial NTP verwenden.

## **5. IP-Netz BSA Backbone**

### **5.1. Sind die Übergabepunkte von den IP-Netz BSA GE zum Backbone IP-Netz BSA festgelegt?**

Ja, die Standorte für den Übergang von der GE zum IP-Netz BSA Backbone sind als Arbeitsversion definiert und werden bis September 2019 durch die Filialen / GE verifiziert und bis Ende Jahr in Zusammenarbeit mit dem ISB/FUB im Detail geplant.

Entsprechende Arbeitsaufträge werden im Juli 2019 an die Filialen erstellt.

### **5.2. Ab wann steht der Backbone IP-Netz BSA zur Verfügung?**

Der Backbone IP-Netz BSA steht ab Ende 2020 zur Migration bzw. Ablösung von VDV bereit.

### **5.3. Was müssen die Filialen/GE für den Backbone IP-Netz BSA zur Verfügung stellen?**

Die Filialen / GE müssen zwei Dinge zuhanden Backbone IP-Netz BSA zur Verfügung stellen:

1. Geeignete technische Räume an den Standorten der Backbone Übergabepunkte (2 pro GE) für die Installation der Netzwerkausrüstung des Bundes
2. LWL-Fasern zur Ergänzung des optischen Backbones des Bundes

Beide Punkte werden im Dokument «2019-07-08\_IPNetzBSA\_AnforderungenIKTRäume» genauer beschrieben.

### **5.4. Wie ist der Übergang zum Backbone technisch realisiert bzw. welche technischen Anforderungen müssen die Router ASTRA-seitig erfüllen?**

Die technische Ausgestaltung der Schnittstelle ist Stand Juli 2019 noch in Diskussion. Die Arbeitshypothese geht von folgenden Annahmen aus:

- Verwendung einer optischen 10GE-Ethernet-Schnittstelle mit einer einfachen BGP-Konfiguration und 802.1ag und/oder BFD zur Fehlererkennung
- Einsatz eines DWDM-Gerätes (OTN) an den BB Standorten ASTRA durch das FUB installiert
- Keine zusätzlichen L3-Router durch das BIT notwendig

### **5.5. Werden die Verbindungen zum Bundesverwaltungsnetz (BV-Netz, Office Netz) bestehen bleiben?**

Ja, alle Verbindungen zum Netz der Bundesverwaltung (BV-Netz) mit den Bundesapplikationen bleiben unverändert bestehen. Obwohl das BV-Netz und das IP-Netz BSA Backbone vom BIT betrieben, handelt es sich um zwei vollständig getrennte Netze.

## **6. IP-Adressierung**

### **6.1. Welche Geräte sollen in einem ersten Schritt auf IPv6 migriert werden?**

Die Migration auf IPv6 soll top-down erfolgen. D.h. in einem ersten Schritt sollen das UeLS und die Abschnittsrechner (AR) in den GE auf IPv6 migriert werden.

Ebenso sollen Anlagen bzw. Geräte, die auf der Managementebene schweizweit benötigt werden, auf IPv6 migriert werden. Dies betrifft also bspw. Kameras.

### **6.2. Dürfen die einzelnen Anlagen in den Abschnitten noch mit IPv4 adressiert werden?**

Ja, sie dürfen noch für bestehende Anlagen. Das Netzwerk wird noch für einige Jahre einen Mischbetrieb IPv4/IPv6 unterstützen müssen. Viele Leitsysteme bzw. Anlagesteuerungen sind heute noch nicht in der Lage, IPv6 zu unterstützen.

Bei künftigen Erneuerungen oder bei Neuinstallationen soll aber darauf geachtet werden, dass die Anlagen dual-stack aufgesetzt werden damit der Übergang auf reines IPv6 vollzogen werden kann. Wenn immer möglich, soll IPv6 eingesetzt werden.

## **7. DNS, DHCP und IP Address Management (IPAM/DDI)**

### **7.1. Wann wird das IPAM-Tool für die GE zur Verfügung stehen?**

Das IPAM-Tool wird ab Ende 2020 für die Nutzung der GE zur Verfügung stehen.

### **7.2. Unterstützt das IPAM-Tool auch die Verwaltung von IPv4?**

Ja, das IPAM-Tool kann neben der IPv6-Verwaltung von jeder GE auch zur Verwaltung von IPv4-Adressen genutzt werden.

Für die Verwaltung von IPv4 werden zentral keine Vorgaben gemacht. Das IPAM-Tool muss aber so genutzt werden wie bereitgestellt und darf nicht individuell angepasst oder erweitert werden. Selbstverständlich können und dürfen die vorhandenen Konfigurationsmöglichkeiten des Tools genutzt werden.

### **7.3. Welche Systeme muss die GE im Bereich IP-Adressvergabe und Namensauflösung aufbauen?**

Die Dokumentation «83041 IP-Netz BSA, technisches Konzept DNS und IP-Adressvergabe» ist aktuell in Bearbeitung und wird im November 2019 in einer Entwurfsversion vorliegen.

Im Hinblick auf die Migrationsplanung kann aber bereits Folgendes gesagt werden:

- Um effizient mit IPv6 umgehen zu können, wird grundsätzlich eine DNS-, DHCPv6 Serverinfrastruktur benötigt. Eine Verbindung zum IPAM-Tool ist zwingend.
- Die Serverinfrastruktur ist durch die GE bereitzustellen.

## **8. Security und Netzwerkzonen**

### **8.1. Werden die Vorgaben Bund in den Sicherheitsrichtlinien ASTRA berücksichtigt?**

Ja, die Vorgaben werden berücksichtigt und in den eigenen Richtlinien ASTRA vertieft bzw. konkretisiert. Insbesondere die Bundesvorgaben SI001, SI002 und SI003 bilden die Basis für die ASTRA Richtlinien.

Die ASTRA Richtlinie 13030 wird in der nächsten Revision insbesondere die SI003 für das ASTRA vorgeben.

### **8.2. Sind künftig lokale Übergänge verboten?**

Nein, die lokalen Netzübergänge müssen aber auf das absolute Minimum begrenzt werden. Das IP-Netz BSA ist nicht das Bundesverwaltungsnetz, sondern ein dediziertes Prozess-Netz und muss deswegen auf die notwendigen Übergänge zu Partnern wie bspw. den Kantonspolizeien eingeschränkt werden. Die Übergänge müssen die Sicherheitsrichtlinie des ASTRA vollumfänglich erfüllen.

### **8.3. Werden im IP-Netz BSA der GE Firewalls zum Backbone IP-Netz BSA eingesetzt?**

Die GE betreiben weiterhin ihre eigenen Netzübergänge hin zum IP-Netz BSA Backbone. Wir gehen davon aus, dass die benötigte Funktionalität gegenüber dem ASTRA-eigenen Backbone (d.h. gegenüber anderen GE, der VMZ und den RZ) im MPLS-Router abgedeckt werden kann (keine stateful Filterfunktionalität notwendig). Den GE steht aber offen, dedizierte Hardware-Firewalls einzusetzen.

### **8.4. Was muss mit den Netzübergängen zu Fremdnetzen und dem Internet angepasst werden?**

Nichts, sofern die Richtlinie 13030 bereits heute eingehalten wird, müssen die bestehenden DMZ nicht angepasst werden.

## **9. Network Access Control**

### **9.1. Ab wann wird das NAC-Tool zur Verfügung stehen?**

Das NAC-Tool wird nicht vor 2021 zur Verfügung stehen.

### **9.2. Wird das NAC-Tool ebenfalls zentral zur Verfügung gestellt?**

Das ist noch abhängig von der Betriebsorganisation. Das NAC-Tool muss getrennt vom eigentlichen Netzbetrieb genutzt werden, d.h. es muss eine eigene Sicherheitsorganisation aufgebaut werden oder zur Verfügung stehen. Ob diese Organisation zentral, regional oder lokal pro GE aufgebaut wird, ist aktuell in Abklärung im Zusammenhang mit der Neubeurteilung der Betriebsorganisation BSA, Aus heutiger Sicht ist eher davon auszugehen, dass ein NAC-Tool gemeinsam für das ganze ASTRA beschafft wird, aber dezentral durch die GE betrieben wird.

Die Dokumentation «83043 IP-Netz BSA: Aufbau und Betrieb Network Access Control» befindet sich in Arbeit und wird Ende 2019 in einem ersten Entwurf zur Verfügung stehen.

## **10. Network Management System**

### **10.1. Wird das NMS auch zentral für den Betrieb in den GE zur Verfügung gestellt?**

Nein, das NMS bleibt vollständig in der Verantwortung der Filialen/GE. Es wird aber verlangt, dass gewisse Funktionen bzw. Arbeitsweisen über das NMS erfolgen (siehe dazu ASTRA Richtlinie 13040).

## **11. Betrieb**

### **11.1. Werden Service Levels einheitlich definiert und vorgegeben?**

Ja, die Service Level Definitionen werden einheitlich für das gesamte IP-Netz BSA festgelegt und schweizweit verwendet.

### **11.2. Werden die Betriebsprozesse für das IP-Netz BSA vorgeschrieben?**

Nein. Jede GE betreibt ihr Netz gemäss den lokalen Prozessen. Es werden aber trotzdem verschiedenen Vorgaben gemacht, die durch die Betriebsorganisationen in den GE einzuhalten sind:

- Zu erfüllende Aufgaben,
- die zu erreichenden Service Levels,
- einzusetzende Tools bspw. IPAM-Tool,
- Skill-Level der Mitarbeitenden.

## **12. Änderungsverzeichnis**

### **12.1. Neu in FAQ V1.3**

Folgende Kapitel wurden ergänzt oder angepasst:

- Kap. 4.7 angepasst
- Französische Version wurde neu erstellt.

### **12.2. Neu in FAQ V1.2**

Folgende Kapitel wurden ergänzt oder angepasst:

- Kap. 4.3
- Kap. 4.9
- Kap. 8.3

### **12.3. Neu in FAQ V1.1**

Folgende Kapitel wurden ergänzt oder angepasst:

- Kap. 2.1 angepasst inkl. der Beilage
- Kap. 4.5 – Kap. 4.8
- Kap. 7.3
- Kap. 8.3 – Kap. 8.4
- Kap. 9.2