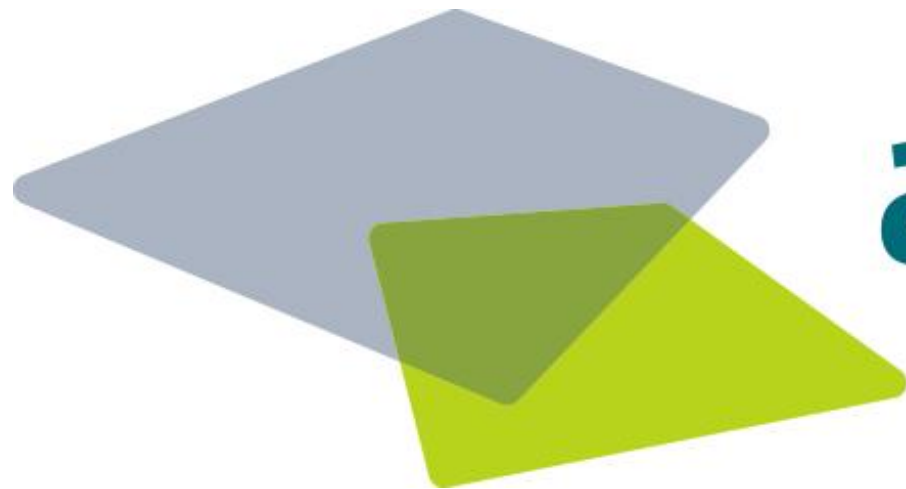




aspectra
hosting your future



aspectra
hosting your future

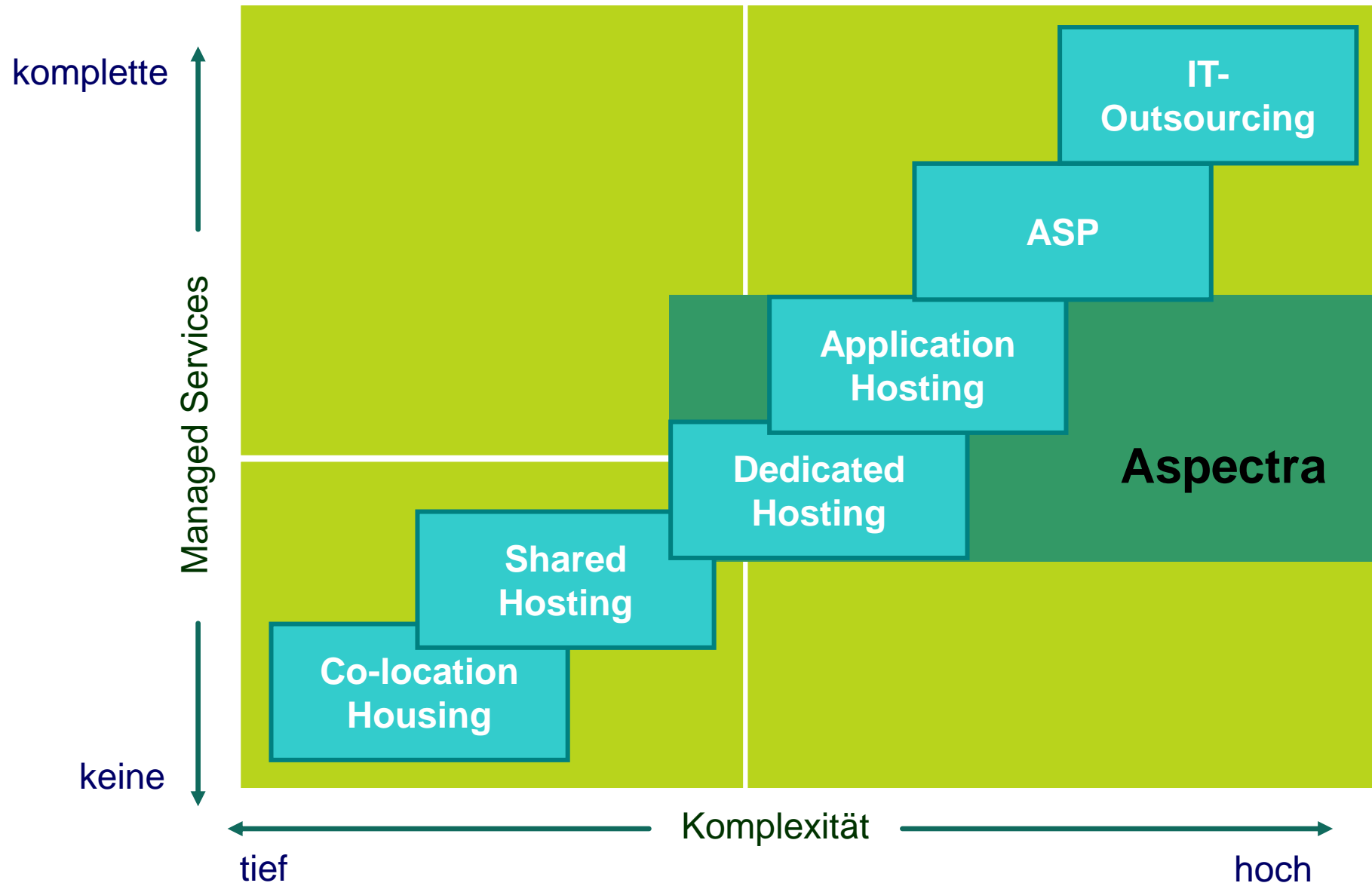
IPv6 - Wie komplex ist es wirklich?



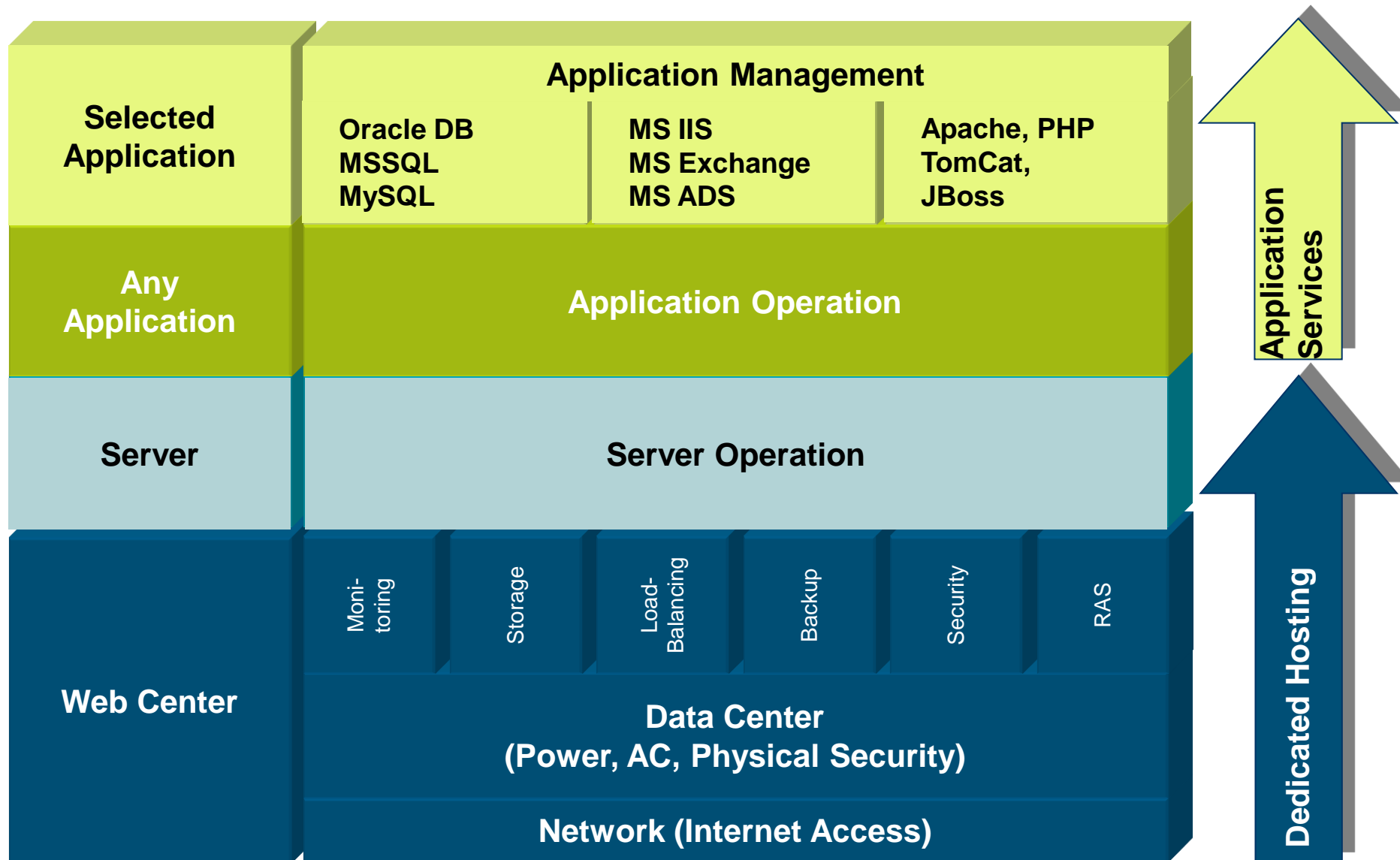
- ❖ Die Motivation
- ❖ Die Strategie
- ❖ Die Implementierung
- ❖ Kritische Würdigung
- ❖ 5 Do's
- ❖ 5 Dont's
- ❖ Pitfalls and Challenges
- ❖ Offene Punkte
- ❖ Q&A

- ❖ **Aspectra**
- ❖ Die Motivation
- ❖ Die Strategie
- ❖ Die Implementierung
- ❖ Kritische Würdigung
- ❖ 5 Do's
- ❖ 5 Dont's
- ❖ Pitfalls and Challenges
- ❖ Offene Punkte
- ❖ Q&A

- ❖ Gegründet 2000
- ❖ Dedizierter Hostler: Jeder Kunde ist in dedizierten Zonen und hat dedizierte Server.
- ❖ Zielgruppe: Hochverfügbar / Hochsicher
- ❖ ISO27001 und FINMA Zertifiziert
- ❖ 2 Datacenter (Glattbrugg, Pratteln)
- ❖ 23 Mitarbeiter



Differenzierung der Hosting-Dienste.



Aspectra's Schichtenmodell.

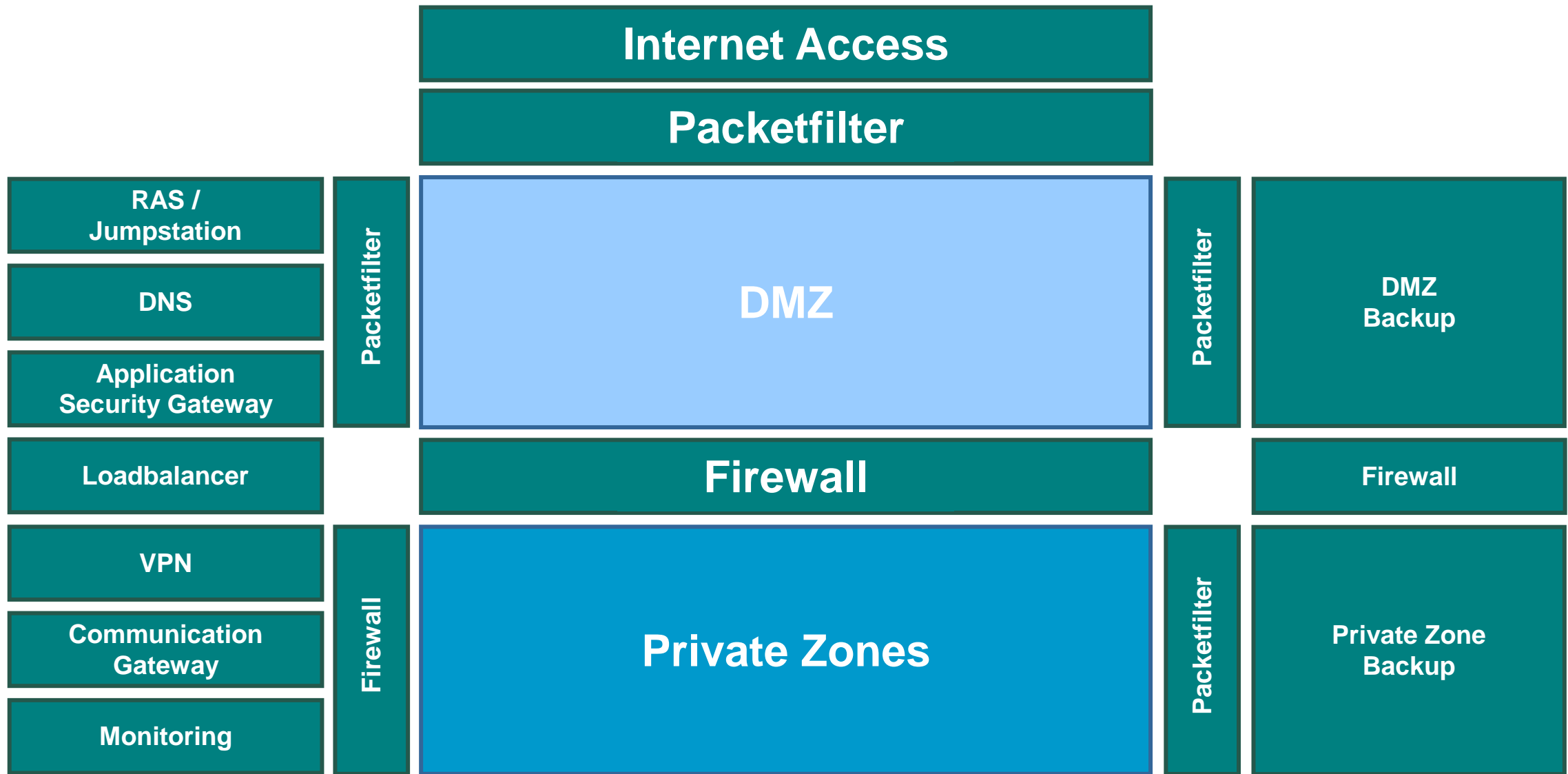
- ❖ Aspectra
- ❖ **Die Motivation**
- ❖ Die Strategie
- ❖ Die Implementierung
- ❖ 5 Do's
- ❖ 5 Dont's
- ❖ Offene Punkte
- ❖ Kritische Würdigung
- ❖ Q&A

- ❖ Dyn.com: The Average US Household uses 5.7 Internet devices (2013)
- ❖ Unzählige Geräte
 - xPhones, xPads, PC, Notebook, Diskstation, Dreambox, Playstation, RasPi, Printer, Powerplug, WLAN Router / Repeater , Telefon, TV, Hifi
- ❖ 31.01.2011 IANA Exhaustion.
- ❖ 04.2012 Aspectra sieht keinen akuten Bedarf. Lass uns spielen
- ❖ 14.09.2012 RIPE Exhaustion

- ❖ Dual Stack Aspectra
- ❖ Ohne Zusatzkosten für den Kunden

- ❖ Wo fängt man an?
 - Ausbildung @ Digicomp
 - Wenige spezifischen Mitarbeiter: Base und Security Team

07.2012 - Ziel



Die Plattform Architektur

- ❖ Provider (Internet Link, BGP, IP Adressen)
- ❖ Netzwerk (Router, DNS, Netzwerkkonzept)
- ❖ Filterstufen (Paketfilter, Firewalls)
- ❖ Monitoring
- ❖ Server und Applikationen

- ❖ Anfrage bei den Providern: Wir hätten gerne IPv6
 - Der zweitgrösste verwies an den Verkäufer. Zu deutsch: Können wir nicht.
 - Der grösste sagte: Können wir, in ca. 3-6 Monaten. Kostet xxxx Fr.
 - Der kleinste sagte: klar, kein Problem, hier der Vertrag.

- ❖ Keine Provider Independent Ranges mehr bei IPv6
 - Das ist ein Problem für einen Hoster wie Aspectra
 - Keine Flexibilität was den Provider angeht
 - Déjà vu: Telenor > Nextra > Solpa > T-Systems > Cablecom > UPC
 - Das ist aber auch eine Chance

- ❖ 9.10.2012 Aspectra wird LIR

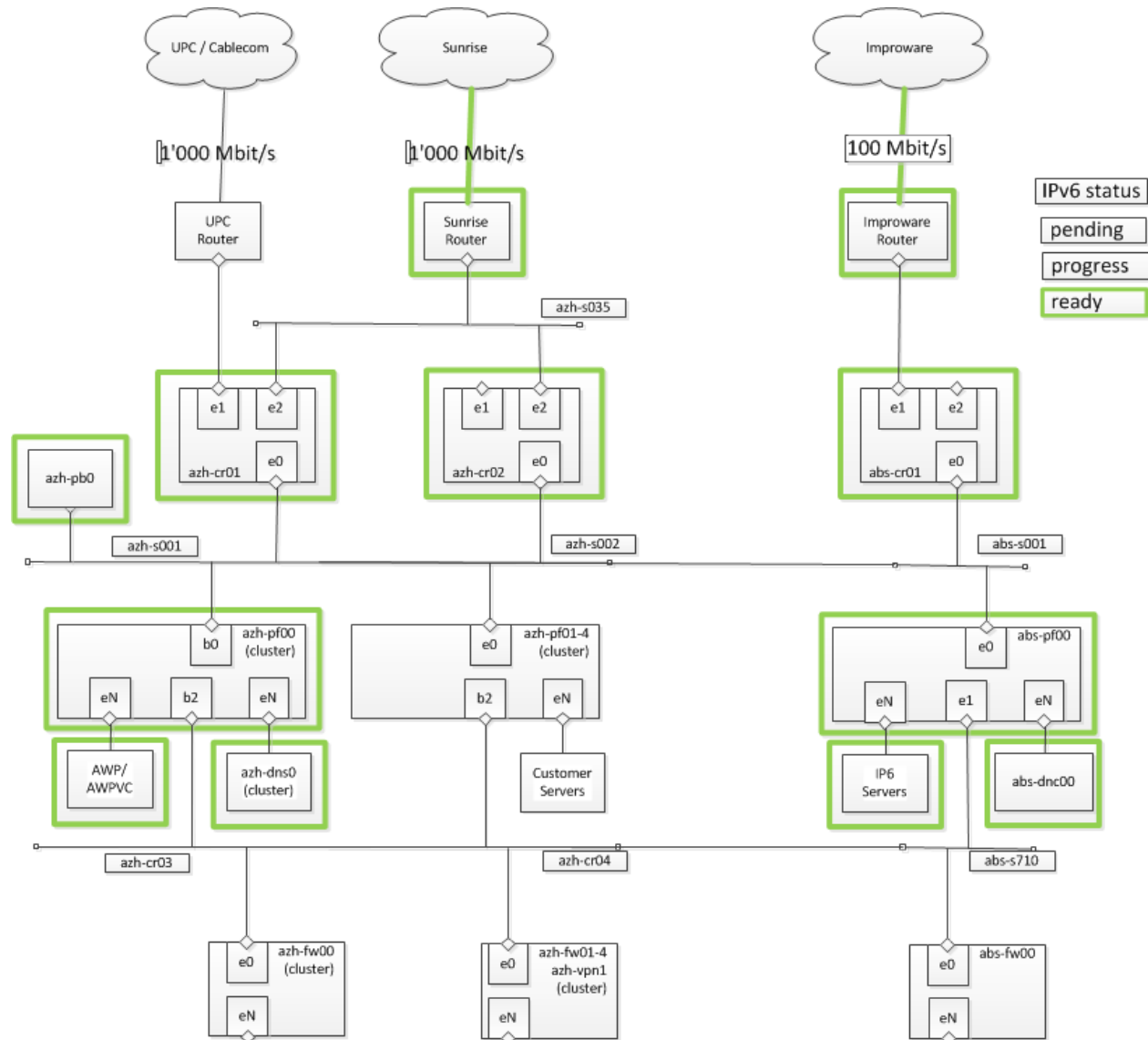
- kriegt `2a02:e0c0::/29`
- besucht entsprechende Kurse

`2a02:e0c0:: - 2a02:e0c7:ffff:ffff:ffff:ffff:ffff:ffff`

- ❖ Bestehendes robustes, flexibles IPv4 und Netzwerkkonzept
 - Mit wenigen Regeln sind werden die Ranges definiert (Netze Kodiert)
 - Über beide RZ verteilt: Layer 3, 450 Zonen, wachsend, z.T. überspannend (Layer 2)
 - Routing zentralisiert

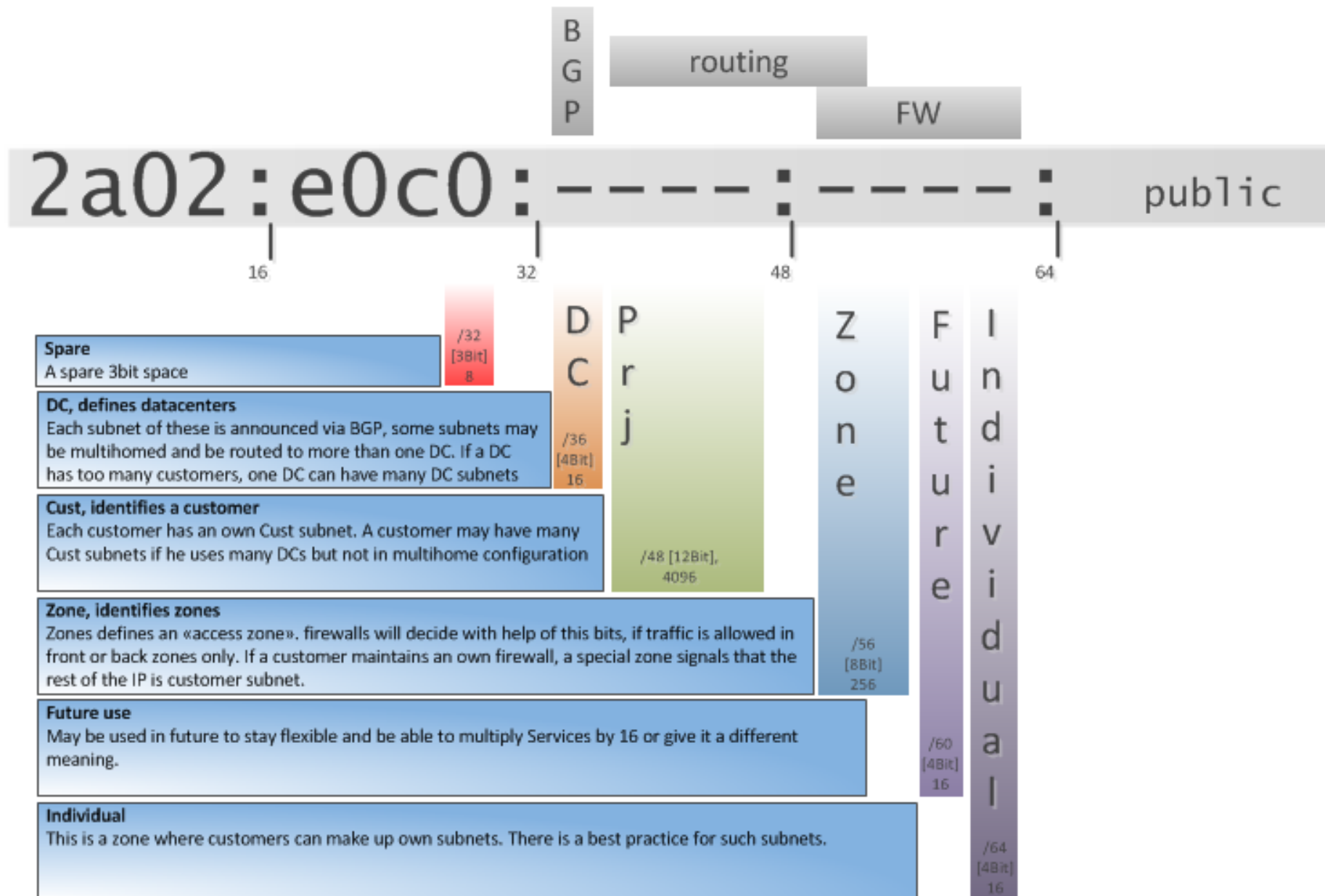
- ❖ Was nun?
 - Wirft man das bestehende Konzept über Board?
 - Lehnt man IPv6 Konzept an IPv4 an?

- ❖ Ziel: So einfach und flexibel wie möglich, Wachstum möglich
 - Hier viel zeit investiert



04.2013 – Netzwerk Konzept III

- ❖ Was macht ein IP Konzept einfach?
- ❖ Was macht der Netzwerk Admin täglich?
 - Verfolgbarkeit eines IP Pakets
- ❖ Bewusster Verzicht auf Hierarchie in unserem AS9100
 - Andere Vorteile wiegen mehr: Verfolgbarkeit eines IP Pakets
- ❖ Bewusstes weglassen von unnötigen Encodierungen in der IPv6 Adresse
 - Schränkt zu fest ein
- ❖ Bewusster Verzicht auf unique local IPv6 Adressen
 - Wenn es nicht geht ohne -> Konzept erweitern
 - We will cross the bridge when we get there...



- ❖ Gewähltes Implementationskonzepte: Edge to Core, Vertikale Integration
- ❖ August 2013
 - Start @ 2nd Site: IPv6 BGP Announcement, router pingable
- ❖ September 2013
 - Schulung für alle Engineers
 - Routing & Firewalls @ 2nd Site
 - Implementation erster Server
- ❖ October 2013
 - Begin DNS
 - Clients IPv6 Range @ Office, Tunnel @ Datacenter
- ❖ November 2013
 - Basic Monitoring, DNS Security and Cleanup
 - Start primary site

❖ Dezember 2013

- Erste vertikale Integration beendet
- Ab 15.12 Christmas freeze
- Eigene Services implementieren: Web Statistik, Homepage, Reverse Proxy, Kundencockpit (Myaspectra.ch)

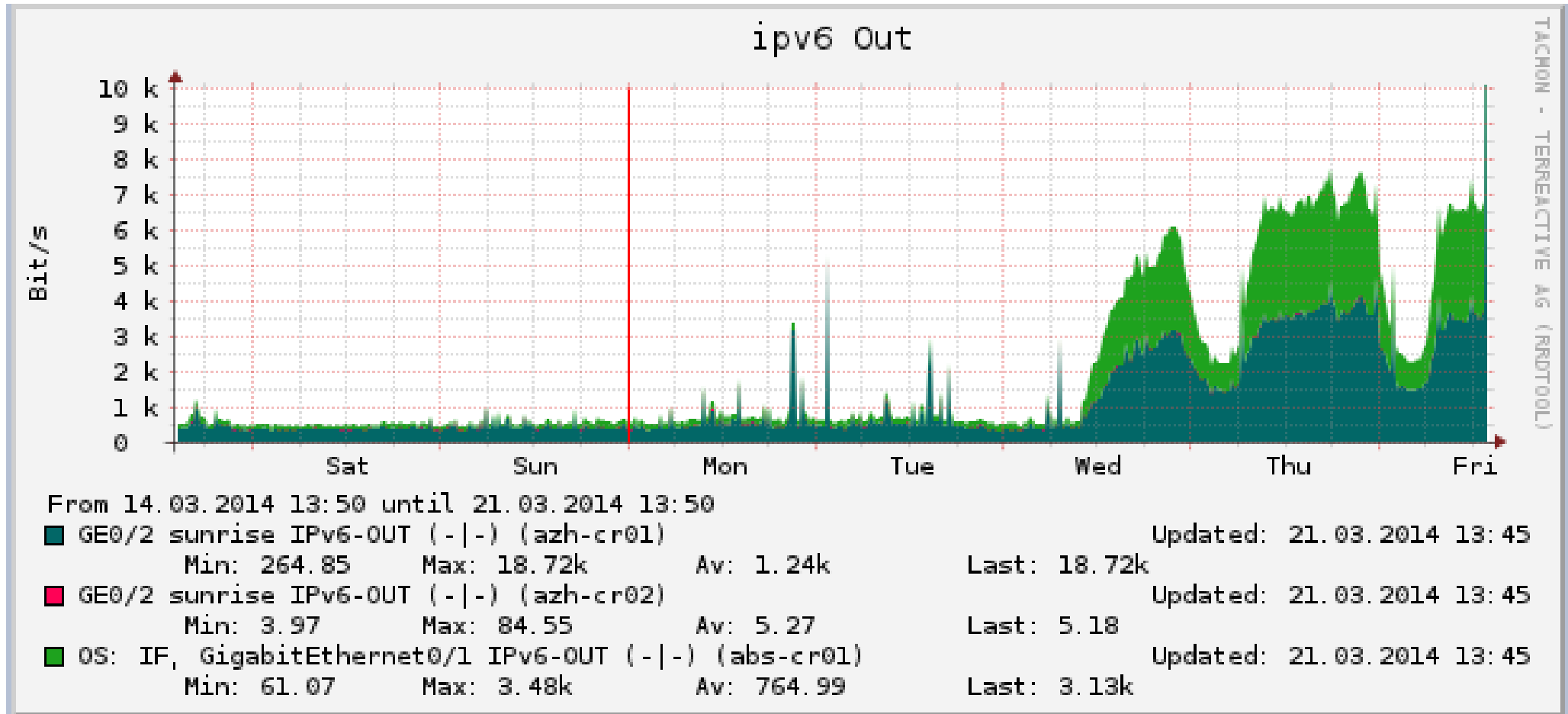
❖ Januar – Februar 2014

- Fehlerbehebung: neue Kernels, neue IOS
- Redundanzen eingeführt: mehrere BGP Anbindungen

❖ 18. März 2014

- IPv6 AAAA für DNS Server eingetragen
- Reverse DNS Zonen bei RIPE aktiviert
- Glue Record
- Abschluss der ersten Integrationsstufe -> IPv6 ist produktiv

- Start: 07.2012
- End: 03.2014



Implementation: 21 Monate für 8kbit/s

❖ Wie komplex?

- IPv6 ist keine Quantenphysik, wacher als bei IPv4 sollte man jedoch sein
- Man beginnt von vorn

❖ Effektiver Nutzen?

Heute:

- Wenig, weil wenige Clients vorhanden
- Wenig, weil wenige Server vorhanden
- Aber morgen.....

- ❖ Dual stack, but with own IPv6 addresses (become a LIR)
- ❖ Find out if your HW can cope with the extra load caused by dual stack
- ❖ Schedule ad-hoc edu/learning
- ❖ Set a top level goal, define scopes, budget, roadmap
- ❖ Invest enough time in the concept and deployment plan for
 - IPv6 addressing
 - routing (BGP)
 - DNS
- ❖ Test, Test, Test in Lab environments, sandbox or at home
- ❖ One thing at a time: Isolated steps (possibly in conjunction with scheduled maintenance activities)

Do...

- ❖ Think you can dual stack in two weeks
- ❖ Overdefine your concept. It will restrict you later
- ❖ Believe manufacturers being IPv6 ready: They will write anything onto the product box just to sell it. Most products have limitations.
- ❖ Buy new hardware just because of IPv6 : Use the regular product life cycle
- ❖ Forget monitoring, logging, security: One for IPv4 and one for IPv6
 - system/network performance
 - E2E scans
 - firewall rules, and logs

Don't...

- ❖ Beware of the DAD (Duplicate Address Detection)
 - On startup the system IPv6 address is setup as 'tentative' until DAD takes place (normally very fast)
 - Some applications can't bind their listener until DAD completes
 - Race condition, application may refuse to start (e.g. DNS 'bind' application)

- ❖ Migration on Live systems
 - Be aware: You are implementing changes on the core of your data center
 - Availability will inevitably decrease before getting better
 - Cisco IOS: Different branches have different features have different bugs
 - New kernels on firewalls:
 - New daemons on DNS Servers: Higher memory consumption

- ❖ Mixing Dual stack and single stack Environments
 - Windows Domains: The Global Catalog will not sync and expire after 60 days in a mixed stack environment. IPv6 is preferred, no fallback.

- ❖ 20% Man Power @ Aspectra
- ❖ Viele Wartungsfenster (Nachtarbeit) an Live Systemen
- ❖ External Man Power: (Security & Netzwerk) terreActive
- ❖ Hardware: 1 WLAN AP

❖ Offene Punkte @ Aspectra

- Implementation auf Kundenzonen und Server
- Ipv6 Monitoring: E2E, Ping, IP Flow Traffic
- VPN
- Private Zonen wo notwendig

❖ Offene Punkte beim Kunden

- Je nach Kunde kann IPv6 nicht implementiert werden

Q&A



Danke für Ihre Aufmerksamkeit.

Ben Mathis

Leiter IT Plattform

www.aspectra.ch

+41 44 296 56 13

ben.mathis@aspectra.ch

Danke

