



IPv6 profile for German public administration (R&D project)

RIPE64 16.04.2012



Dipl. Ing. Tahar Schaa

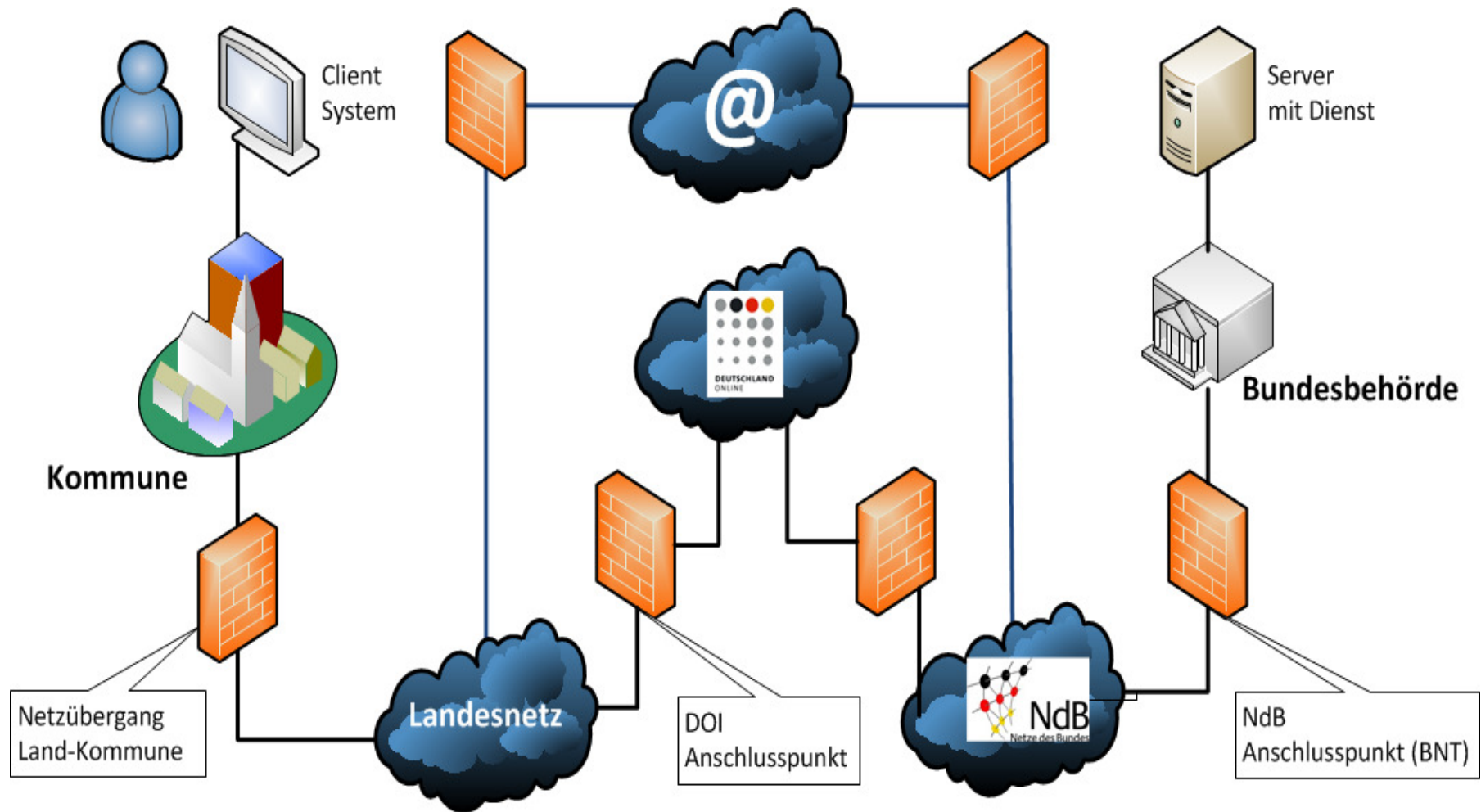
Tel +49 (0) 151 11 44 38 75

Mail tahar.schaa@cassini.de

Initial position

- **Grown IT-infrastructure with internal IPv4-adresses (10.0.0.0/8)**
- **Overlapping internal address spaces overall public organizations**
- **Public administration organizations need NAT44 several times to communicate with each other**
- **Common services**
 - E-Mail
 - Web
 - E-government process workflows
- **Currently marginally in use**
 - VoIP
 - Videoconferencing
- **IPv6 not in use**

Overview - Schema



IPv6 preparation part I

Address space

○ IPv6 address space (::/26) for German public administration

- Global Unicast
- ISP independent
- Central management

○ Local Internet Registry (LIR) „de.government“

- Ministry of interior
- Bundesverwaltungsamt

○ IPv6-addressframework nationwide for

- Federal government
- Federal states
- Municipalities

Block	Nr.	Dual	Präfix	Block	Nr.	Dual	Präfix
00: Hamburg	0	000000	2a02:1000 /32	08: Niedersachsen	8	001000	2a02:1008 /32
01: Reserve	1	000001	2a02:1001 /32	09: Reserve	9	001001	2a02:1009 /32
02: Schleswig Holstein	2	000010	2a02:1002 /32	10: Reserve	10	001010	2a02:100a /32
03: Reserve	3	000011	2a02:1003 /32	11: Reserve	11	001011	2a02:100b /32
04: Bremen	4	000100	2a02:1004 /32	12: NRW Land	12	001100	2a02:100c /32
05: Reserve	5	000101	2a02:1005 /32	13: Reserve	13	001101	2a02:100d /32
06: Mecklenburg-Vorpommern	6	000110	2a02:1006 /32	14: NRW Kommunen	14	001110	2a02:100e /32
07: Reserve	7	000111	2a02:1007 /32	15: Reserve	15	001111	2a02:100f /32
Block	Nr.	Dual	Präfix	Block	Nr.	Dual	Präfix
16: Hessen	16	010000	2a02:1010 /32	24: Saarland	24	011000	2a02:1018 /32
17: Reserve	17	010001	2a02:1011 /32	25: Reserve	25	011001	2a02:1019 /32
18: Reserve	18	010010	2a02:1012 /32	26: DOI+Öffentliche	26	011010	2a02:101a /32
19: Reserve	19	010011	2a02:1013 /32	27: Reserve	27	011011	2a02:101b /32
20: Rheinland-Pfalz	20	010100	2a02:1014 /32	28: Sachsen	28	011100	2a02:101c /32
21: Reserve	21	010101	2a02:1015 /32	29: Reserve	29	011101	2a02:101d /32
22: Reserve	22	010110	2a02:1016 /32	30: Reserve	30	011110	2a02:101e /32
23: Reserve	23	010111	2a02:1017 /32	31: Reserve	31	011111	2a02:101f /32
Block	Nr.	Dual	Präfix	Block	Nr.	Dual	Präfix
32: Brandenburg	32	100000	2a02:1020 /32	40: Baden Württemberg	40	101000	2a02:1028 /32
33: Reserve	33	100001	2a02:1021 /32	41: Reserve	41	101001	2a02:1029 /32
34: Berlin	34	100010	2a02:1022 /32	42: Reserve	42	101010	2a02:102a /32
35: Reserve	35	100011	2a02:1023 /32	43: Reserve	43	101011	2a02:102b /32
36: Sachsen-Anhalt	36	100100	2a02:1024 /32	44: Bayern	44	101100	2a02:102c /32
37: Reserve	37	100101	2a02:1025 /32	45: Reserve	45	101101	2a02:102d /32
38: Thüringen	38	100110	2a02:1026 /32	46: Reserve	46	101110	2a02:102e /32
39: Reserve	39	100111	2a02:1027 /32	47: Reserve	47	101111	2a02:102f /32
Block	Nr.	Dual	Präfix	Block	Nr.	Dual	Präfix
48: Netze des Bundes	48	110000	2a02:1030 /32	56: BMVg res.	56	111000	2a02:1038 /32
49: Netze des Bundes	49	110001	2a02:1031 /32	57: BMVg res.	57	111001	2a02:1039 /32
50: Netze des Bundes	50	110010	2a02:1032 /32	58: BMVg res.	58	111010	2a02:103a /32
51: Netze des Bundes	51	110011	2a02:1033 /32	59: BMVg res.	59	111011	2a02:103b /32
52: Reserve	52	110100	2a02:1034 /32	60: BMVg	60	111100	2a02:103c /32
53: Reserve	53	110101	2a02:1035 /32	61: BMVg	61	111101	2a02:103d /32
54: Vorreserviert	54	110110	2a02:1036 /32	62: BMVg	62	111110	2a02:103e /32
55: Reserve	55	110111	2a02:1037 /32	63: BMVg	63	111111	2a02:103f /32

Now we've got IPv6 addresses....

But what next?

Are the responsible public officers ready

to introduce IPv6?
to procure IPv6?

No! They need help!

Difficulties to introduce IPv6

Procurement

- Public tenders require IPv6 for years – Bidders are offering “some” IPv6 for years
- There are no detailed IPv6 specs for procurement
- Implementations where not useable in “real networking life”

Migration

- IT responsible persons shrink back from IPv6 migration from the scratch without a receipt
- Best practices adapted for German public administration are requested
- “Making something (IPv6) means you could make mistakes. Perhaps its better to keep IPv4 forever?” – Guidelines are needed

IPv6 preparation part II

IPv6 R&D project for German public administration

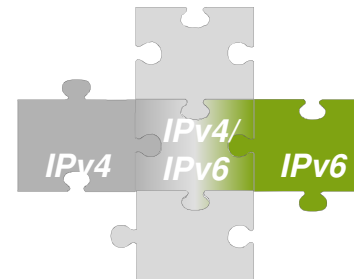
IPv6-Profil

- IPv6-Profil-matrix for components
- IPv6-Profil-matrix for applications
- IPv6-Profil-description

IPv6-Knoten				
Grund-Anforderungen				
Profil		RFC 2460	IPv6 Basic Specification	✓
			Ignorieren des 'Flow Label'-Feldes	✓
	ICMP			
		RFC 4443	ICMPv6	✓

Migration support

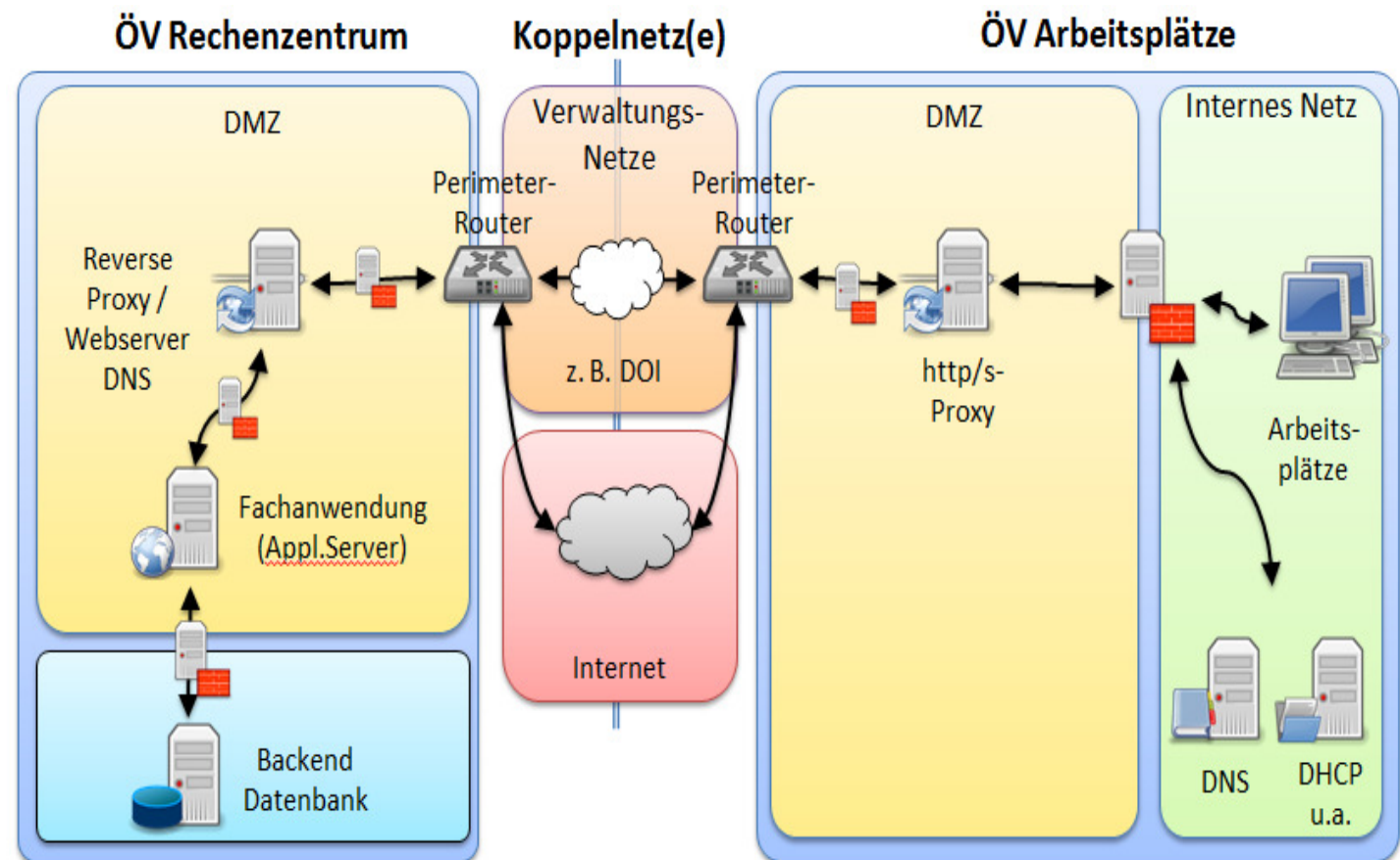
- IPv6 Migration guideline
- IPv6 Workshop slides
- IPv6 Migration checklists



What to migrate?

Which components need profiles?

- segments
 - provider
 - consumer
 - transfer networks
 - Coupling networks
- Security zones
- Validity zones for internal IPv4 addresses

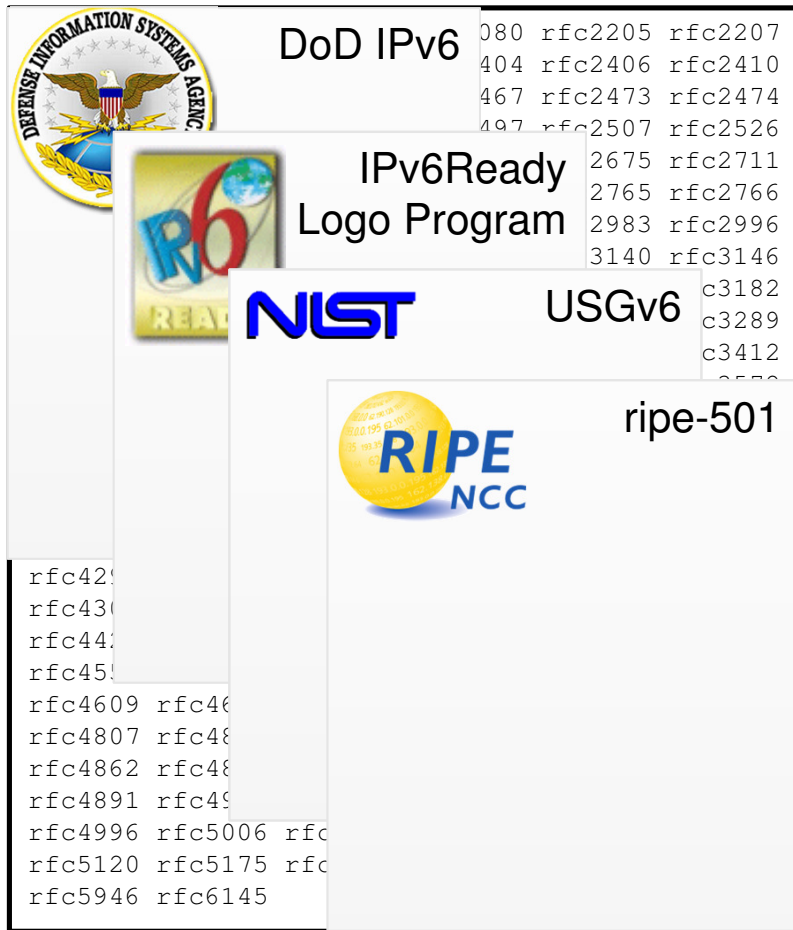


IPv6 profile – too much IETF RFCs

```
rfc1772 rfc1981 rfc1997 rfc2080 rfc2205 rfc2207
rfc2210 rfc2401 rfc2402 rfc2404 rfc2406 rfc2410
rfc2451 rfc2460 rfc2464 rfc2467 rfc2473 rfc2474
rfc2475 rfc2491 rfc2492 rfc2497 rfc2507 rfc2526
rfc2545 rfc2590 rfc2597 rfc2671 rfc2675 rfc2711
rfc2740 rfc2746 rfc2747 rfc2750 rfc2765 rfc2766
rfc2784 rfc2872 rfc2918 rfc2961 rfc2983 rfc2996
rfc2998 rfc3086 rfc3095 rfc3097 rfc3140 rfc3146
rfc3152 rfc3168 rfc3173 rfc3175 rfc3181 rfc3182
rfc3226 rfc3241 rfc3246 rfc3247 rfc3260 rfc3289
rfc3306 rfc3307 rfc3315 rfc3392 rfc3411 rfc3412
rfc3413 rfc3414 rfc3484 rfc3526 rfc3566 rfc3572
rfc3596 rfc3602 rfc3633 rfc3686 rfc3736 rfc3775
rfc3810 rfc3843 rfc3879 rfc3936 rfc3948 rfc3956
rfc3963 rfc3971 rfc3972 rfc3986 rfc4007 rfc4022
rfc4038 rfc4087 rfc4106 rfc4113 rfc4191 rfc4193
rfc4213 rfc4271 rfc4282 rfc4283 rfc4291 rfc4292
rfc4293 rfc4294 rfc4295 rfc4301 rfc4302 rfc4303
rfc4306 rfc4307 rfc4308 rfc4309 rfc4338 rfc4360
rfc4362 rfc4429 rfc4434 rfc4443 rfc4495 rfc4541
rfc4543 rfc4552 rfc4581 rfc4594 rfc4601 rfc4604
rfc4607 rfc4609 rfc4632 rfc4659 rfc4718 rfc4760
rfc4798 rfc4807 rfc4809 rfc4815 rfc4821 rfc4835
rfc4861 rfc4862 rfc4864 rfc4868 rfc4869 rfc4877
rfc4884 rfc4891 rfc4941 rfc4944 rfc4945 rfc4966
rfc4995 rfc4996 rfc5006 rfc5063 rfc5072 rfc5095
rfc5114 rfc5120 rfc5175 rfc5308 rfc5340 rfc5350
rfc5555 rfc5946 rfc6145
```

- 165 „standard“-RFCs about IPv6
- >300 RFCs mentioning IPv6
 - ongoing development
- Defined keywords for "requirement levels" (RFC 2119)
 - "MUST"
 - "MUST NOT"
 - "REQUIRED"
 - "SHALL"
 - "SHALL NOT"
 - "SHOULD"
 - "SHOULD NOT"
 - "RECOMMENDED"
 - "MAY"
 - "OPTIONAL"

Other IPv6 profiles



DoD IPv6

IPv6Ready Logo Program

NIST

USGv6

ripe-501

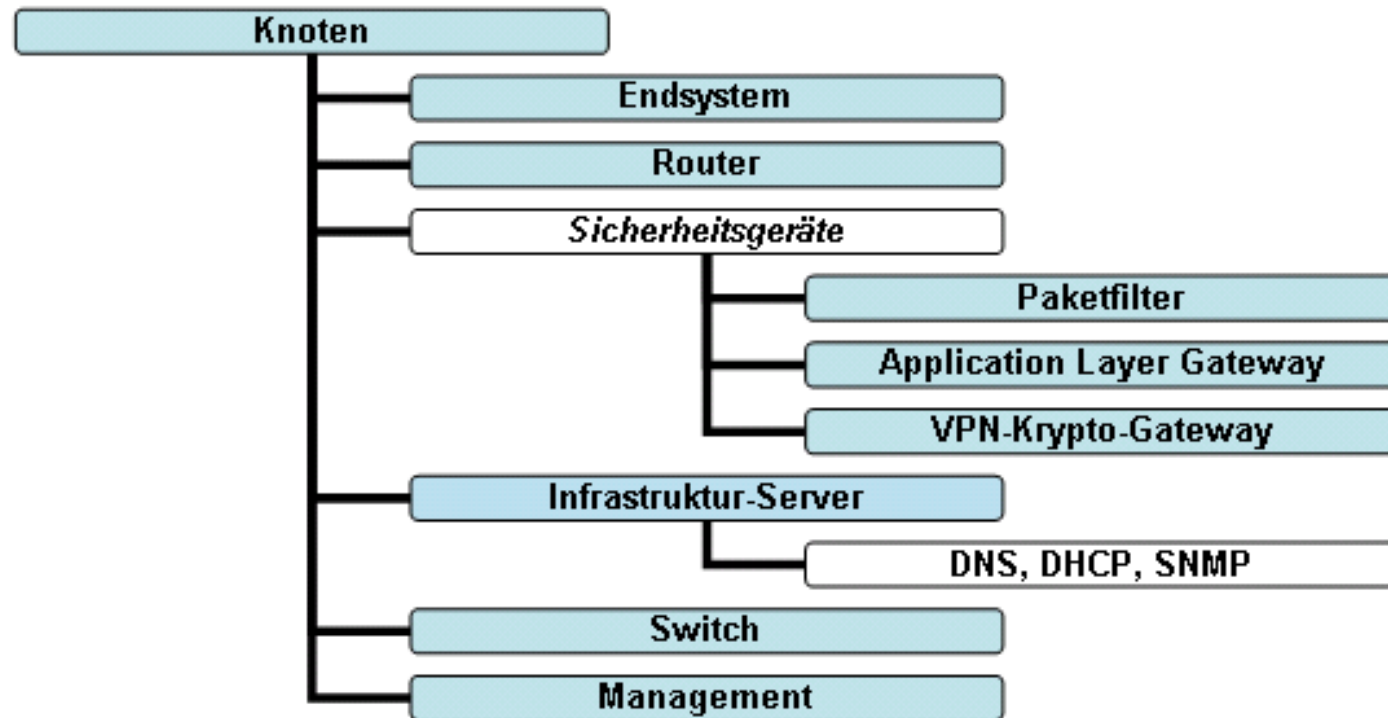
RIPE NCC

080 rfc2205 rfc2207
404 rfc2406 rfc2410
467 rfc2473 rfc2474
497 rfc2507 rfc2526
2675 rfc2711
2765 rfc2766
2983 rfc2996
3140 rfc3146
c3182
c3289
c3412
c3550

rfc4241
rfc4301
rfc4443
rfc4575
rfc4609 rfc4690
rfc4807 rfc4853
rfc4862 rfc4892
rfc4891 rfc4919
rfc4996 rfc5006 rfc5015
rfc5120 rfc5175 rfc5286
rfc5946 rfc6145

- **ripe-501**
 - "mandatory"
 - "optional"
 - "if X is requested, equipment must support Y"
- **NIST USGv6**
 - Device Taxonomy: Host, Router, Network Protection Device
 - Functional Categories of IPv6 Capabilities
 - Individual Device Profiles
- **IPv6Ready Logo Programm**
 - Compliance certification
- **DoD Profile, UCR 2008, Change 2**
 - Fokus on security

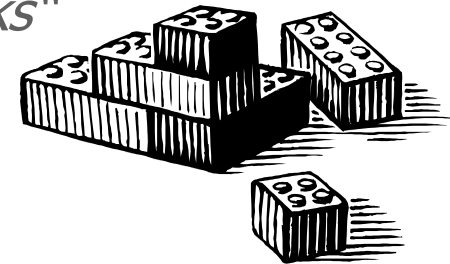
IPv6 profile device classes



IPv6 profile – sort by funktions

- Communication
 - Base requirements
 - ICMP, Transfer
 - Addressing
 - format, semantic
- DNS-client
- Migration mechanisms
- IP-security
- Multicast
- QoS
- MobileIP

„Building blocks“



IPv6 node functions

- Optional: Network management
- Local management funktions

seperate: management

IPv6 profile for components

Kategorie	Kategorie	Kategorie	RFC	Titel	Merkmal, Funktion	Projekt-Empfehlung	Kommentar	ripe-501	NIST	ipv6ready.org	RFC 6434 - IPv6 Node Requirements	US DoD UCR 2008 Change 2 / IPv6 Standard Profiles
Gesamter Gerätetyp												
Kommunikation des IPv6-Knotens												
Grund-Anforderungen												
Basis												
	RFC 2460	IPv6 Basic	verpflichtend		Nicht-Nutzung und Ignorieren von Feldern	verpflichtend		verpflichtend	verpflichtend	Core	verpflichtend	verpflichtend
	RFC 6437	IPv6 Flow Label Specification	verpflichtend			verpflichtend					empfohlen für Quell-Endsystem	nicht erwähnt (jünger als Profil-Dokumente)
	RFC 5722	Handling of Overlapping IPv6 Fragments	verpflichtend			verpflichtend					verpflichtend	nicht erwähnt
ICMP												
	RFC 4443	ICMPv6	verpflichtend			verpflichtend		verpflichtend	verpflichtend	Core	verpflichtend	verpflichtend
		Konfigurierbarkeit der Erzeugung von 'Destination Unreachable'	verpflichtend			verpflichtend	DoS-Angriff durch übermäßige, nicht zustellbare Nachrichten möglich				UCR, Kap. 5.3.5, Req. 14.2	verpflichtend
		Konfigurierbarkeit der Beantwortung von 'echo request'-Nachrichten an Multicast- und Anycast-Adressen	verpflichtend			verpflichtend	DoS-Angriff durch übermäßige 'echo request'-Nachrichten möglich				UCR, Kap. 5.3.5, Req. 14.3	verpflichtend
	RFC 5095	Revised ICMPv6	optional			optional		optional	verpflichtend	Core	verpflichtend	verpflichtend
	RFC 4884	Extended ICMPv6 for multi-part messages	optional			optional		optional	empfohlen		optional	empfohlen
Neighbor Discovery												
	RFC 4861	Neighbor Discovery	verpflichtend			verpflichtend		verpflichtend	verpflichtend	Core	empfohlen	verpflichtend
		Nicht-Setzen des 'Override Flag'	verpflichtend			verpflichtend						verpflichtend
		Verwerfen von 'Neighbor Advertisement'-Nachrichten, für die kein Ziel-Eintrag im 'Neighbor Cache' vorhanden ist	verpflichtend			verpflichtend						verpflichtend
		Verwerfen von 'Neighbor Advertisement'-Nachrichten im 'Neighbor Cache INCOMPLETE'-Zustand	verpflichtend			verpflichtend						verpflichtend
		Verwerfen von 'Neighbor Cache'-Einträgen, für die 'Address Resolution' fehlschlägt	verpflichtend			verpflichtend						verpflichtend
	RFC 5942	IPv6 Subnet Model	empfohlen			empfohlen	Ergänzung zu RFC 4861				empfohlen	nicht erwähnt (jünger als Profil-Dokumente)
wenn SEND eingesetzt werden soll						empfohlen		optional				

German profile for public sector

comparison to other profiles

Unified structure

Summary

Kommunikation
Grundanforderungen
Adressierung
DNS-Klient
Migrationsmechanismen
IP-Sicherheit
Multicast
Dienstgüte / QoS
Mobilität
Optional: Netzwerk-Management
Geräte Funktionen

Knoten
Router / Layer-3 Switches
Endsystem
Layer-2 Switch
Netzwerk-Sicherheit
Infrastrukturserver

rfc1772	rfc1981	rfc1997	rfc2080	rfc2205	rfc2207
rfc2210	rfc2401	rfc2402	rfc2404	rfc2406	rfc2410
rfc2451	rfc2460	rfc2464	rfc2467	rfc2473	rfc2474
rfc2475	rfc2491	rfc2492	rfc2497	rfc2507	rfc2526
rfc2545	rfc2590	rfc2597	rfc2671	rfc2675	rfc2711
rfc2740	rfc2746	rfc2747	rfc2750	rfc2765	rfc2766
rfc2784	rfc2872	rfc2918	rfc2961	rfc2983	rfc2996
rfc2998	rfc3086	rfc3095	rfc3097	rfc3140	rfc3146
rfc3152	rfc3168	rfc3173	rfc3175	rfc3181	rfc3182
rfc3226	rfc3241	rfc3246	rfc3247	rfc3260	rfc3289
rfc3306	rfc3307	rfc3315	rfc3392	rfc3411	rfc3412
rfc3413	rfc3414	rfc3484	rfc3526	rfc3566	rfc3572
rfc3596	rfc3602	rfc3633	rfc3686	rfc3736	rfc3775
rfc3810	rfc3843	rfc3879	rfc3936	rfc3948	rfc3956
rfc3963	rfc3971	rfc3972	rfc3986	rfc4007	rfc4022
rfc4038	rfc4087	rfc4106	rfc4113	rfc4191	rfc4193
rfc4213	rfc4271	rfc4282	rfc4283	rfc4291	rfc4292
rfc4293	rfc4295	rfc4301	rfc4302	rfc4303	rfc4306
rfc4307	rfc4308	rfc4309	rfc4338	rfc4360	rfc4362
rfc4429	rfc4434	rfc4443	rfc4495	rfc4541	rfc4543

IPv6 matrix for applications

			Benötigte Funktionen / Komponenten	Struktur			Server			Sicherheit				Netzinfrastruktur		
				Endsystem	Unterstützende Systeme	Server	Webserver	Datenbank	...	Proxy	Paketfilter (PF)	VPN	...	DNS	DHCP	...
Betrachtete Anwendung / Komponente																
		Produkt														
Anwendung																
Web-basiert																
			MESO													
Endsystem (Beschreibung der Rolle)																
Stationärer Desktop																
			Windows 7													
			Linux Ubuntu 4.10													
Mobiler Desktop (WLAN)																
Mobiler Desktop (Mobilfunk)																
Server																
Webserver																
			Apache 2.0.14													
Datenbank																
			ORACLE Version 11g Release 1													
			SQL-Server 2005													
Sicherheitskomponenten																
Proxy																
Packetfilter																
VPN																

Endsystem	(PF, Proxy)	Webserver, Datenbank	X	X		(X)	(X)	(X)		X	-						
Stationärer Desktop	(PF, Proxy)	Anwendungs-server, Datenbank	X	X		(X)	(X)	(X)		X	-						
			(Proxy, PF)						(X)			(X)		X	DHCP(X)		
			(Proxy, VPN, PF)						(X)			(X)	(X)	X	X		
			(Proxy, PF) VPN						(X)			(X)	X	X			
			(Proxy, PF) DNS			(Datenbank)			(X)				(X)	(X)	X	-	

Softwarematrix: Example

			Benötigte Funktionen / Komponenten	Struktur			Server			Sicherheit				Netzinfrastruktur		
				Endsystem	Unterstützende Systeme	Server	Webserver	Datenbank	...	Proxy	Paketfilter (PF)	VPN	...	DNS	DHCP	...
Betrachtete Anwendung / Komponente																
Anwendung		Produkt														
	Web-basiert	VISkompakt	Endsystem	(PF, Proxy)	Webserver, Datenbank	X	X		(X)	(X)	(X)		X			
			Stationärer Desktop	(PF, Proxy)	Anwendungs-server, Datenbank	X	X		(X)	(X)	(X)		X			
Endsystem (Beschreibung der Rolle)																
	Stationärer Desktop	Windows 7		(Proxy, PF)					(X)	(X)			X	DHCP(X)		
		Linux Ubuntu 4.10														
	Mobiler Desktop (WLAN)			(Proxy, VPN, PF)					(X)	(X)	(X)		X	X		
	Mobiler Desktop (Mobilfunk)			(Proxy, PF) VPN					(X)	(X)	X		X			
Server																
	Webserver	Apache 2.0.14		(Proxy, PF)	(Datenbank)		(X)		(X)	(X)			X			
			DNS													
	Datenbank		ORACLE Version 11g Release 1											X		
			SQL-Server 2005													
Sicherheitskomponenten																
	Proxy															
	Paketfilter															
	VPN															

DHCP(x) - DHCP-Client, wenn DHCP verwendet wird

Comments? Questions?

Cassini Consulting GmbH
Technology Guidance

Halskestraße 46

40880 Ratingen

Germany

visit www.cassini.de



Dipl. Ing. Tahar Schaa

Tel +49 (0) 151 11 44 38 75

Mail tahar.schaa@cassini.de