



PROFILE BEI IPv6

HILFEN IM RFC-DSCHUNGEL

Uwe Kaiser, 24. November 2014

REFERENZ-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 ...
```

- 232 Standards RFCs zu IPv6 (Request For Comments)
- 200 weitere RFCs mit Bezug zu IPv6
 - weiter dynamische Entwicklung
- Definierte Terminologie für Anforderungen (RFC 2119)
 - "MUST"
 - "MUST NOT"
 - "REQUIRED"
 - "SHALL"
 - "SHALL NOT"
 - "SHOULD"
 - "SHOULD NOT"
 - "RECOMMENDED"
 - "MAY"
 - "OPTIONAL"

EXISTIERENDE PROFILE



ripe-501



USGv6



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
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		

IPv6Ready
Logo
Program



DoD IPv6



VERSCHIEDENE PROFILE – VERSCHIEDENE SCHWERPUNKTE



DoD IPv6

IPv6Ready Logo Program

NIST USGv6

ripe-554

rfc42...
rfc43...
rfc44...
rfc45...
rfc4609 rfc46...
rfc4807 rfc48...
rfc4862 rfc48...
rfc4891 rfc49...
rfc4996 rfc5006 rfc...
rfc5120 rfc5175 rfc...
rfc5946 rfc6145

- **ripe-554 (Nachfolger von 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 Program**
 - Zertifizierung von Konformität
- **DoD Profile, UCR 2008, Change 2**
 - Schwerpunkt: Sicherheit

Anforderungen an IPv6-ICT-Ausrüstung in Form von Profilen

Beschreibt Best Common Practices (BCP)

Die Basis für ripe-554 sind die verschiedenen RFCs,
NIST-Dokumente und das IPv6Ready-Programm



Profile für folgende Hardware-Klassen:

- Endgerät
- Layer-2-Switch, Router und CPE-Router
- Sicherheitskomponenten:
Paketfilter, Application-Layer-Gateways und Intrusion-Prevention-Geräte
- Mobile Devices
- Load Balancer



Nachfolger von ripe-501 – ripe-501 hat weite Beachtung gefunden

DoD IPv6 PROFILE



Department of Defense
Unified Capabilities Requirements 2008, Change 2
Version von 2010

Aufteilung in die Produktklassen: Host, Router, Layer-3-Switch,
Network Appliance, Security Device, Advanced Server
Kategorien: MUST, SHOULD, SHOULD+ (wird verpflichtend)



„Konfiguration“ von Netzwerkkomponenten und
Verschärfung der Anforderungen aus RFCs



Teil von DoD IPv6 Generic Test Plan

- Test von Konformität, Interoperabilität und Leistung von Produkten

IPv6-READY LOGO PROGRAMM



Internationales Testprogramm

Soll die RFC-Konformität von Komponenten und die Interoperabilität zwischen Komponenten von verschiedenen Herstellern gewährleisten.

Drei Phasen werden unterschieden:

- Phase 1: Silbernes Logo – IPv6 Kernprotokolle werden unterstützt (Phase 1 ist offiziell abgeschlossen)
- Phase 2: Goldenes Logo – Phase-2-Anforderungen, bestehend aus 450 Einzeltests
- Phase 3: entspricht Phase-2-Spezifikationen plus IPsec als verpflichtend



! Obwohl es IPv6Ready-Testcenter gibt, dürfen die Tests von den Herstellern selbst durchgeführt werden

<http://www.ipv6ready.org/>

NIST hat für die US Regierung (USG) Profile erstellt
Unterstützung der US-Bundesämter bei der Einführung von IPv6

Basis für die NIST-Profiles sind die IPv6-RFCs der IETF
Profile für Hosts, Router und Netzwerk-Sicherheitskomponenten



Funktionale IPv6-Kategorien:

- Basis-Anforderungen
- Routing-Protokolle
- QoS
- Transition Mechanisms
- Addressing
- IP Security
- Network Management
- Multicast
- Mobility
- Application Requirements



IETF RFC 6434 - IPv6 NODE REQUIREMENTS



Auflistung von Anforderungen an einen IPv6-Knoten

- IPv6-Knoten (Node): Gerät, das IPv6 nutzt
- IPv6-Router: Ein Knoten, der Pakete weiterleitet
(nicht an ihn selbst adressiert)
- IPv6-Host: Jeder Knoten, der kein Router ist



Inhalt: Aktuelle Auflistung von RFCs (RFC 6434: Dezember 2011)

Gute, lesbare Übersicht über die wichtigsten Dinge

Tipp: Nutzung von <http://tools.ietf.org/html/rfc4294>

- Updates und Berichtigungen werden gleich dargestellt

PROFILENTWICKLUNG





DoD IPv6

080	rfc2205	rfc2207
404	rfc2406	rfc2410
467	rfc2473	rfc2474
497	rfc2507	rfc2526
2675	rfc2711	
2765	rfc2766	
2983	rfc2996	
3140	rfc3146	
	c3182	
	c3289	
	c3412	
	c5550	



IPv6Ready
Logo Program



USGv6



ripe-554

rfc42		
rfc43		
rfc44		
rfc45		
rfc4609	rfc46	
rfc4807	rfc48	
rfc4862	rfc48	
rfc4891	rfc49	
rfc4996	rfc5006	rfc
rfc5120	rfc5175	rfc
rfc5946	rfc6145	



Vereinheitlichung der Struktur



Einordnung der Profile



**Ableitung eines IPv6-Profiles
für die Öffentliche Verwaltung**

ZIEL DER PROFILE:



Identifikation von notwendigen, empfohlenen und optionalen Funktionen für IPv6-(Dual-Stack-)Betrieb

- Unterstützung von Ausschreibungen und Beschaffung
- Unterstützung der Analyse von vorhandener Infrastruktur in Hinblick auf eine wirtschaftlich sinnvolle Migration

Besonderheit: Ganzheitliche Sicht

- von Anfang bis Ende (vom Arbeitsplatz bis zur Fachanwendung)
- über alle Schichten (von Netzwerkkomponenten bis zur Software)

„IPv6-Profil für die Öffentliche Verwaltung“ bestehen aus

- IPv6-Profiltabellen (inkl. Profil-Beispielen zur Erläuterung)
- Begleitenden Erläuterungen zum IPv6-Profil und Anforderungen an Softwarekomponenten
- Software-Matrix zur Erfassung von Software-Abhängigkeiten

STRUKTUR DER PROFILE

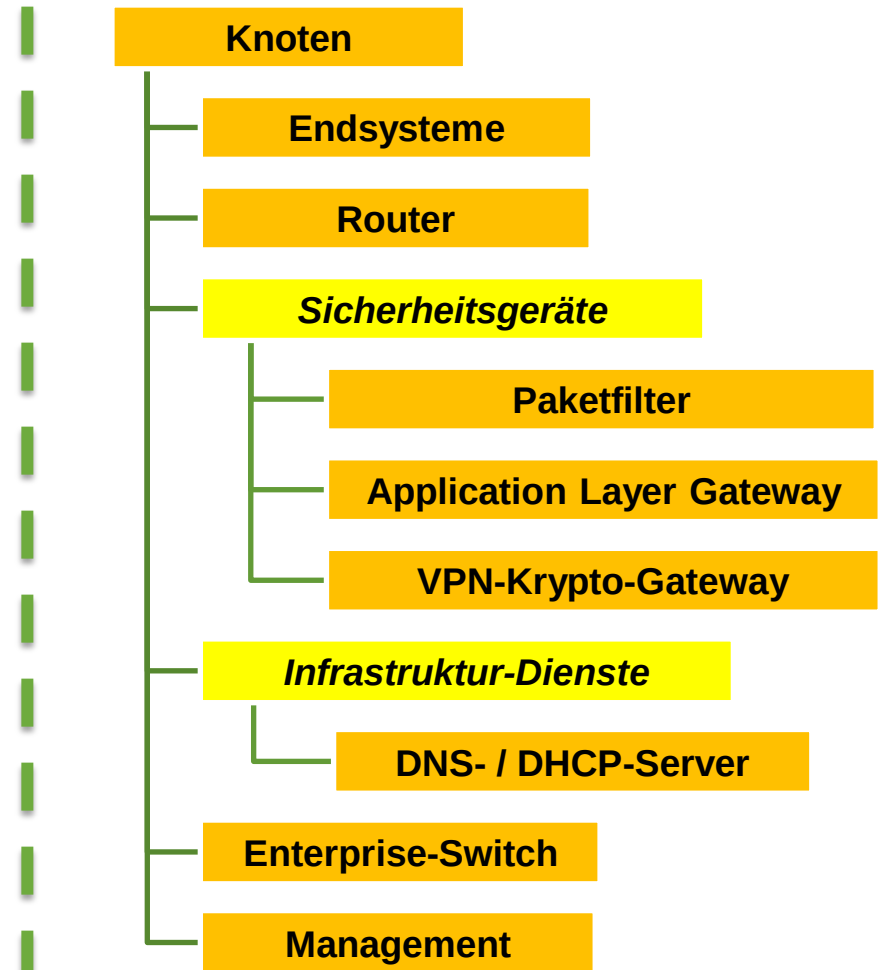


■ Kommunikation

- Grundanforderungen
 - ICMP
 - Transfer
- Adressierung
 - Konfiguration
 - bei Verwendung von SLAAC
 - bei Verwendung von DHCP
- Transitionsmechanismen
- IP-Sicherheit
- Multicast
- QoS
- Mobilität

■ Optional: Netzwerk-Management

■ Gerätefunktionalität



Kate- gorie	Kate- gorie	Kate- gorie	RFC	Titel	Merkmal, Funktion	Projekt-Empfehlung	Kommentar	ripe-501
Gesamter Gerätetyp								
Kommunikation des Endsystems								
Grund-Anforderungen								
s. a. Knoten								
Neighbor Discovery								
s. a. Knoten								
	RFC 4861	Neighbor Discovery			Konfigurierbarkeit zum Ignorieren von Redirect-Nachrichten	verpflichtend	s. Knoten	
					Akzeptieren von Redirect-Nachrichten nur vom zuständigen Router für das Ziel	verpflichtend	sicherheitsrelevant	
					Bevorzugung von erreichbaren Routern	verpflichtend	sicherheitsrelevant	
	RFC 4311	IPv6 Host-to-Router Load Sharing				optional		
Transfer								
s. a. Knoten								
	RFC 4821	Packetization Layer Path MTU Discovery				empfohlen		optional
Adressierung								
Allgemein								
s. a. Knoten								
	RFC 3484	Default Address Selection				verpflichtend	s. Knoten	
					Bereitstellung einer konfigurierbaren Regeltabelle zum Überschreiben der Default Address Selection	empfohlen	je nach Schutzbedarf auch "verpflichtend"	
Konfiguration								
					Unterstützung von manueller / statischer Adresskonfiguration	verpflichtend	s. Knoten	
					Unterstützung von Autokonfiguration (SLAAC und DHCPv6 (stateful und stateless))	verpflichtend		
SLAAC							Für hinreichend große Netze Verwendung von DHCP empfohlen	
s. a. Knoten								
	RFC 4941	SLAAC Privacy Extensions				verpflichtend		optional
	RFC 5453	Reserved IPv6 Interface Identifiers				verpflichtend		

BESONDERHEITEN DES IPv6-PROFILS



Kategorie	Kategorie	Kategorie	RFC	Titel	Merkmal, Funktion	Projekt-Empfehlung	Kommentar	ripe-554 (Nachfolge von ripe-501)	NIST	ipv6ready.org	RFC 6434 - IPv6 Node Requirements	US DoD UCR IPv6 Standard
Gesamter Gerätetyp												
Kommunikation des IPv6-Knotens												
Grund-Anforderungen												
Basis												
			RFC 2460	Internet Protocol, Version 6 (IPv6)	Flow Label Feld wird nicht genutzt und ignoriert (solange RFC 6437 nicht implementiert ist)	verpflichtend		verpflichtend	verpflichtend	Core	verpflichtend	UCR, Kap. 5.3.5, Req. 2 UCR, Kap. 5.3.5, Req. 7
			RFC 6540	IPv6 Support Required for All IPv6-Enabled Nodes		verpflichtend						
			RFC 6437	IPv6 Flow Label Specification		empfohlen					empfohlen	
			RFC 5722	Handling of Overlapping IPv6 Fragments		verpflichtend	überlappende IPv6-Fragmente sind verboten, Errata berücksichtigen!				verpflichtend	
ICMP												
			RFC 4443	ICMPv6		verpflichtend		verpflichtend	verpflichtend	Core	verpflichtend	UCR, Kap. 5.3.5, Req. 14 UCR, Kap. 5.3.5, Req. 14.2
					Konfigurierbarkeit des Antwortverhaltens mit 'Destination Unreachable'	verpflichtend	DoS-Angriff durch übermäßige, nicht zustellbare Nachrichten					UCR, Kap. 5.3.5, Req. 14.3
					Konfigurierbarkeit des Antwortverhaltens mit 'Echo Request'-Nachrichten an Multicast- und Anycast-Adressen	verpflichtend	DoS-Angriff durch übermäßige 'echo Request'-Nachrichten					UCR, Kap. 5.3.5, Req. 2
			RFC 5095	Deprecation of Type 0 Routing Home-Address		verpflichtend		verpflichtend	verpflichtend	Core	verpflichtend	UCR, Kap. 5.3.5, Req. 2
			RFC 4884	Extended ICMP for multi-part messages		optional		optional	empfohlen		optional	IPv6 Standard Profiles, Kap. 2.1
Neighbor Discovery												
			RFC 4861	Neighbor Discovery		verpflichtend		verpflichtend	verpflichtend	Core	empfohlen	UCR, Kap. 5.3.5, Req. 11 UCR, Kap. 5.3.5, Req. 11.1
					Nicht-Setzen des 'Override Flag' für Solicited Advertisements von Anycast- und Proxy-Adressen	verpflichtend	Verschärfung des RFCs, Erhöhung der Sicherheit gegen böswillige Nachbarn					UCR, Kap. 5.3.5, Req. 11.3
					Verwerfen von 'Neighbor Advertisement'-Nachrichten, für die kein Ziel-Eintrag im 'Neighbor Cache' vorhanden ist	verpflichtend	Erhöhung der Sicherheit gegen böswillige Nachbarn: Eintragung nur, wenn Kommunikation mit dem Nachbarn gewünscht					UCR, Kap. 5.3.5, Req. 11.4
					Verwerfen von 'Neighbor Advertisement'-Nachrichten im 'Neighbor Cache'	verpflichtend						UCR, Kap. 5.3.5, Req. 11.5
					Verwerfen von 'Neighbor Cache'-Einträgen, für die 'Address Resolution' fehlschlägt	empfohlen						UCR, Kap. 5.3.5, Req. 12.1
					Managed address configuration'-Flag und 'Other stateful configuration'-Flag dauerhaft	empfohlen						
			RFC 5942	IPv6 Subnet Model		empfohlen	Ergänzung zu RFC 4861				empfohlen	
SEND, wenn Einsatz geplant						empfohlen	nur wenige		optional		optional	

Eigenes Profil
für die ÖV

Gegenüberstellung
der Profile

Vereinheitlichte
Struktur

- Identifikation aller betroffenen bzw. abhängigen Komponenten für den IPv6-Betrieb
- Sichtweise auf Komponenten kann verschieden sein, je nach Stand der Migration oder Zuständigkeit (Grad der Detaillierung)
- Beispiel: Eine Anwendung braucht einen Webserver
 - Webserver als monolithische Komponente, wenn Webserver schon auf IPv6 migriert oder von dritter Seite bereitgestellt
 - Webserver als Komponente steht in Verbindung mit Paketfiltern, ggf. Reverse Proxy, DNS nötig usw.
- Ende-zu-Ende-Sicht von Anwendungsszenarien oder dem Einsatzbereich von Einzelkomponenten
 - Auf welchen anderen Komponenten basiert das Szenario?
 - Welche Abhängigkeiten bestehen zu anderen Komponenten?

SOFTWAREMATRIX



notwendige
Komponenten...

		Zu untersuchende Anwendung		
		Produkt	Version	IPv6 ?
Unterstützende Software	Anwendungs-architektur	Terminal-Service		
		Virtualisierung		
	Generische Anwendungen	Web Application Server		
		Groupware/ATV		
		E-Mail MTA		
		Datenbank-Server		
		Webserver		
		Print Server		
		File Server		
	Anwendungs-Unterstützung	PKI		
		RADIUS		
		Directory Server		
	Frameworks / Middleware	J2EE		
		.NET		
	Betriebssystem			
	Middle Boxes	Firewall		
		ALG		
		VPN Server		
		Load Balancer		
	Netz-Infrastruktur	DNS		
		DHCP		

... für eine
Anwendung

PROFILE TO GO



News Events Pilots Monitoring Publications Partners

 http://www.gen6-project.eu/fileadmin/GEN6/GEN6_PU_D2_4_v1.0.pdf



Das BVA Die BIT IT-Leistungen IT-Themen Ansprechpartner Meldungen



  [STARTSEITE BVA](#) ▶ [THEMENPORTAL BIT](#) ▶ [IT-LEISTUNGEN](#) ▶ [BERATUNGSLEISTUNGEN](#) ▶ [IPV6](#) ▶ [BEST PRACTICE](#)

http://www.bva.bund.de/DE/Organisation/Abteilungen/Abteilung_BIT/Leistungen/IT_Beratungsleistungen/IPv6/best_practice/bestpractice_node.html

Fraunhofer FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin, Germany

www.fokus.fraunhofer.de

Uwe Kaiser

uwe.holzmann-kaiser@fokus.fraunhofer.de
Tel. +49 (0)30 3463-7217