SIEMENS

Industrial Ethernet

IPv6 in der Automatisierungs-technik

White Paper

Ausgabe 06/2019

siemens.de/industrial-ethernet

Inhaltsverzeichnis

IPv6 in der Automatisierungstechnik

1. Grundlagen und Einsatz von IPv6
Die Bedeutung des Internet Protocol Version 6 (IPv6) wird nicht zuletzt aufgrund der Verknappung von IPv4-Adressen zunehmen. Weltweit eindeutige IP-Adressen und die damit einhergehende Möglichkeit, Anlagen und Produktionsstätten global nahtlos zu vernetzen, wird dazu führen, dass IPv6 in den nächsten Jahren nach und nach Einzug in IT und OT-Infrastrukturen halten wird. Neben technischen Grundlagen erhalten Anwender mit den Beispielen ab dem Kapitel 5 auch konkrete Hilfestellungen für den Einsatz der neuen Technologie.

2. IPv6 für die Automatisierungstechnik
Mit der Einführung von IPv6 in der Automatisierungstechnik werden die bisherigen IPv4 Adressen mit 32 Bit auf eine viermal so breite Adresse mit 128 Bit erweitert. Dadurch wird der Adressraum massiv vergrößert und erlaubt zugleich eine komplette Abkehr der bisher eingeführten Adressumsetzungen durch den begrenzten IPv4-Adressraum. Somit ist zukünftig wieder eine problemlose Kommunikation direkt zwischen Endsystemen möglich, eine komplizierte und fehleranfällige Adressdefinition via Network Address Translation (NAT) wird obsolet. In der Zukunft wird es nur noch zu einer reinen „end-to-end"-Kommunikation kommen. Einschränkende Technologien wie NAT/PAT sind nicht mehr erforderlich.

Welchen Anwendernutzen erreicht man mit der Einführung der neuen IPv6-Technologie?

- Durchgängige Diagnose von der ERP Ebene über die Leitebene bis in die Feldebene
- Hierarchischer Aufbau von Netzstrukturen
- Optimiertes Routing

Neue Techniken der IT werden ausschließlich auf IPv6 basieren. Zugleich ist eine Koexistenz von IPv4 zu IPv6 lange zu berücksichtigen. Es ist heute nicht mehr die Frage ob ein Übergang von IPv4 nach IPv6 stattfindet, sondern wann!

Zukünftig wird auf der ERP-Ebene IPv6 vorherrschend sein, da neue Funktionen innerhalb der Software gleich auf den IPv6 Diensten aufsetzen werden.

Durch die zunehmende Verzahnung der Automatisierung mit der Unternehmens-IT werden IPv6 basierende Kommunikationsdienste für eine durchgängige Diagnose auch für Automatisierungsgeräte immer wichtiger.

3. Grundlagen von IPv6

3.1 Wendepunkt/Ausgangslage
Am 1. Februar 2011 war es soweit: Die Internet Assigned Numbers Authority (IANA) vergab den letzten freien Adressblock an das Asia-Pacific Network Information Center (APNIC). Damit sind keine freien IPv4 Adressen mehr zur Zuteilung an die fünf Regionalen Internet Registry (RIR) mehr möglich. Diese können nur noch die letzten beim RIR verbliebenen IPv4 Adressen an ihre Kunden weiter vergeben.

Für die Nutzer des Internet Protokolls IPv4 beginnt damit ein Umstieg auf das bereits seit über 20 Jahren definierte Protokoll IPv6. Die Betriebssysteme wie WINDOWS, Mac OS X oder LINUX bieten bereits seit Jahren hierzu die entsprechende Unterstützung an.

Da mittelfristig weltweit über IPv4 keine Erreichbarkeit mehr gegeben ist, ist der einzige Ausweg aus dieser Misere die Verwendung von global eindeutigen IPv6 Adressen, um wieder die „end-to-end"-Kommunikation sicher zu stellen.

Um ein Gefühl für die Dynamik zu erhalten, welche in den letzten Jahren eingesetzt hat, hier einige Anhaltspunkte aus der Telekommunikation und öffentlichen Netzwerken.

Seit dem „World IPv6 Launch" in 2012, hat sich das IPv6 Datenaufkommen der großen US Mobilfunk Provider innerhalb von vier Jahren auf über 50% gesteigert.

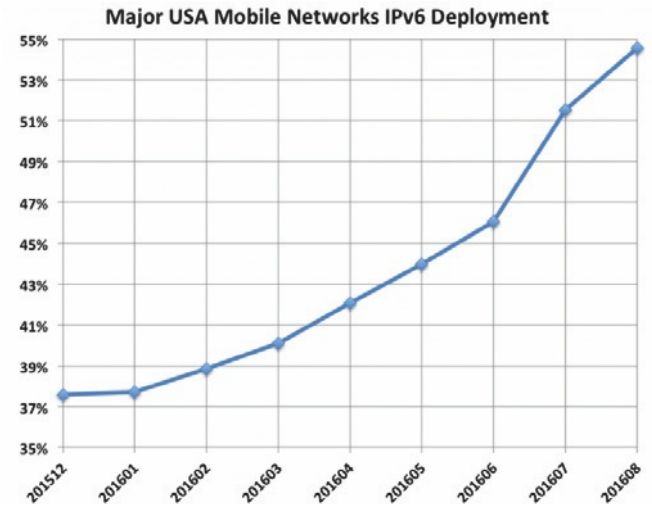


Bild 1: Anstieg IPv6 Datenaufkommen bei den großen Mobilfunk-Providern
Quelle: **https://www.worldipv6launch.org/major-mobile-us-networks-pass-50-ipv6-threshold/**

IPv6 in der Automatisierungstechnik

Für öffentliche Netzwerke ist ein mögliches Analyseverfahren, die Informationen aus der BGP (Border Gateway Protocol) Tabelle der Router auszuwerten und diese ins Verhältnis zu bringen, siehe Bild 2.

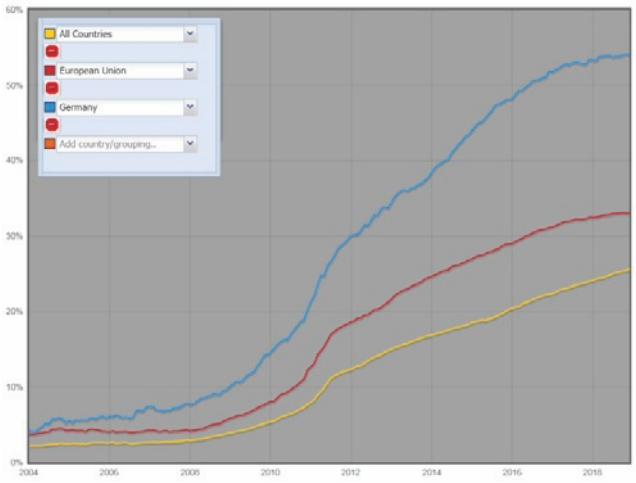


Bild 2: Anstieg IPv6 Router, weltweit (gelb), europäische Union (rot) und Deutschland (blau)
Quelle: **http://v6asns.ripe.net/v/6?s=_ALL;s=_RIR_RIPE_NCC**

Alle Auswertungen weltweit zeigen einen signifikanten Anstieg der IPv6 Kommunikation in den letzten vier Jahren. In einigen Ländern, wie z.B. in Brasilien ist heute eine Telekommunikation über LTE nur noch mit IPv6 „Support" möglich. Geräte mit einer reinen IPv4-Kommunikation werden nicht mehr zugelassen.

3.2 Standardisierung

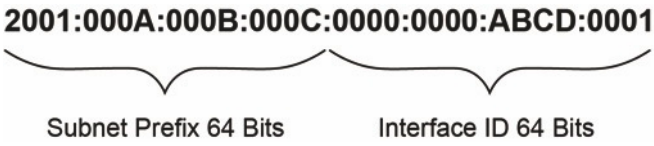
Die Standardisierung, welche im Jahre 1998 mit dem RFC 2460 als offiziellen Nachfolger des IPv4 Protokolls begann ist heute in einem stabilen Zustand. Viele Erweiterungen, wie die Koexistenz von IPv4/IPv6, DHCPv6, Neighbor Discovery u.v.m. sind in der Zwischenzeit in den verschiedenen RFCs beschrieben. Für tiefer gehende Informationen werden die folgenden RFCs empfohlen:

- RFC 3315, Dynamic Host Configuration Protocol for IPv6
- RFC 4291, IP Version 6 Addressing Architecture
- RFC 4294, IPv6 Node Requirements
- RFC 4862, IPv6 Stateless Address Autoconfiguration
- RFC 4861, Neighbor Discovery for IP version 6

3.2.1 Adressaufbau IPv6

Die IPv6-Adressen werden –anders als bei IPv4 – in 8 x 16 Bit Feldern zu je vier Hexadezimalen-Ziffern geschrieben. Diese werden jeweils durch einen Doppelpunkt voneinander getrennt. Es gibt immer eine Subnet Prefix aus 64 Bits und eine Interface ID aus 64 Bits.

Ein Beispiel dafür wäre eine Globale IPv6 Adresse in der folgenden Schreibweise:



Rein rechnerisch sind dadurch 340.282.366.920.938.463. 463.374.607.431.768.211.456 Adressen möglich. Diese unvorstellbar große Zahl kann man nur mit einem einigermaßen erfassbaren Vergleich darstellen, indem man jedem Proton im Universum eine eigene IP Adresse oder für jeden Quadratmeter der Erdoberfläche 6,5x10²³ Adressen zuweisen könnte.

Verdeutlichung des Adressraumes:

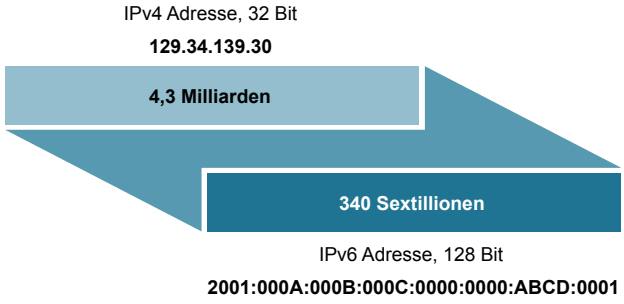


Bild 3: Größe des IP-Adressraums

Damit genug eineindeutige Adressen vorhanden sind, um eine eindeutige Adressierung und damit eine direkte Verbindung zwischen den Teilnehmern zu ermöglichen, entfällt die Notwendigkeit des Network Address Translation (NAT) oder auch des Port Address Translation (PAT).

IPv6 in der Automatisierungstechnik

3.2.2 Viele Adressen an einem Interface

Mit der IPv6 Adressierung erhält jedes Netzwerkinterface mindestens eine, meist jedoch mehrere Adressen. Dies können neben der für die Adressvergabe wichtigen Link Local Address (LLA, wird immer pro Interface automatisch gebildet) auch eine Unique Local Address (ULA) sein oder gleich eine Globale Address (GA) beinhalten.

Hinweis:
Mit der von jedem Gerät automatisch erzeugten LLA, welche immer eindeutig ist, sind alle Geräte im lokalen Subnetz IPv6-technisch erreichbar. Die Geräte sind damit immer erreichbar und diagnostizierbar.

Eine manuelle Konfiguration oder sonstige Einstellung der IPv6-Adresse ist nicht notwendig!

Weiterführende Infos hierzu findet man auch in dem RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Archi-tecture.

3.2.3 IPv6 Adressvergabe

Eine der wichtigsten Neuerungen bei IPv6 ist die automatische Adressvergabe. Mit Hilfe der Autokonfiguration kann sich jeder IP-Knoten selbst eine eindeutige Link-Local Adresse erzeugen ohne hier auf eine manuelle Konfiguration oder einen DHCP Server zurückgreifen zu müssen.

Bei zusätzlicher Benutzung von Router Discovery werden:

- weitere IPv6 Adressen
- Router Adressen
- weitere Konfigurationsparameter

dem Teilnehmer mitgeteilt. Damit möchte man besonders den Aufwand bei der Administration von Netzwerken deutlich reduzieren, siehe Bild 4.

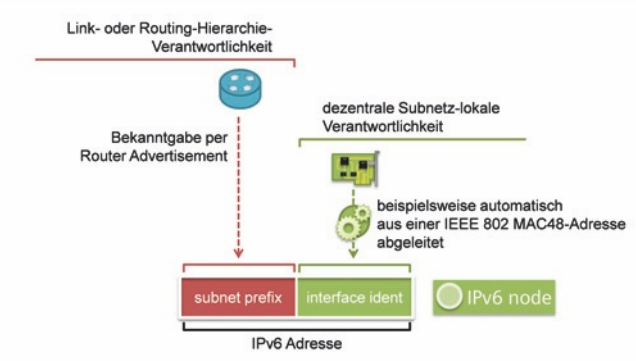


Bild 4: Aufteilung IPv6 Adresse

3.2.4 Dual Stack

Der Begriff Dual Stack bezieht sich in der Regel auf eine vollständige Duplikation der IPv4 und IPv6 Stacks über alle Ebenen im Protokollstapel, von der Anwendungs- bis zur Netzwerkschicht. Der Dual Stack Ansatz stellt sicher, dass die weiterentwickelten Komponenten immer über IPv4 mit nur-IPv4-Komponenten zusammenarbeiten können. In der Automatisierungstechnik wird darüber die Kompatibilität zu bereits vorhandenen Anlagenteilen sichergestellt.

3.2.5 Wesentliche Unterschiede IPv4 / IPv6

Inhalt	IPv4	IPv6
Veröffentlichung	1981 (RFC 791)	1998 (RFC 2460)
Verfügbarer Adressraum	32 Bit, $4{,}29 \times 10^9$ Adressen	128 Bit, $3{,}4 \times 10^{38}$ Adressen
Adressformat	Dezimal: 192.168.1.1	Hexadezimal: 2a00:ad80::0123
Loopback-Adresse	127.0.0.1	1
IPsec-Header	optional	immer vorhanden
Fragmentierung	Host und Router	nur Endpunkt der Kommunikation
Checksum im Header	ja	nein
Optionen im Header	ja	nein
Link-layer address resolution	ARP (Broadcast)	Multicast Neighbor Discovery messages
Router Discovery	optional	zwingend erforderlich
IP-Konfiguration	manuell, DHCP	automatisch, DHCPv6, manuell

Bild 5: Tabelle IPv4/IPv6 Unterschiede

4. Investitionsschutz

Die Einführung von IPv6 wird im Wesentlichen aus der Notwendigkeit getrieben, dass der Adressbereich des globalen IP-Netzes (Internet) ausgeschöpft ist. Ein erweiterter Adressraum wurde mit IPv6 schon vor vielen Jahren definiert, um diese Verknappung zu lösen.

Daher wird die Umsetzung der neuen Adressierung vorrangig den Backbone-Bereich eines Unternehmens berühren und zu einem späteren Zeitpunkt nach und nach über die IT Infrastruktur bis zur Automatisierungsebene wandern.

Dieser Umstieg wird längere Zeit in Anspruch nehmen und es auch erforderlich machen, dass beide Verfahren parallel existieren.

IPv6 in der Automatisierungstechnik

Ein zusätzlicher IPv6 Support bei neuen Geräten sorgt für die problemlose globale Erreichbarkeit ohne Auswirkungen auf die bestehenden Kommunikationsbeziehungen.

Der gleichzeitige Betrieb von IPv4- und IPv6 Kommunikation (siehe Kap. 3.2.4, Dual Stack) erfordert aus Netzwerksicht vor allem Unterstützung in den Layer 3 Geräten (Routing). Vorhandene Layer 2 Geräte (Switches) erlauben zwar prinzipiell sowohl IPv4 als auch IPv6 Kommunikation, zur uneingeschränkten Unterstützung von IPv6 sind allerdings auch auf dieser Ebene Anpassungen nötig.

Durch diese Zweigleisigkeit ist ein Bestandsschutz für Altanlagen vorhanden, eine Umrüstung oder Hochrüstung nur eine Ausnahme.

5. Beispiel: OPC Server

Bei der Verwendung des OPC-Servers von Siemens ist es bereits heute möglich über IPv6 zu kommunizieren. Der OPC Server übernimmt hier die Rolle eines Proxy, welcher einen komfortablen Zugriff auf die Automatisierungsdaten über IPv4 und IPv6 anbietet. Damit wird es den OPC Clients (HMI/SCADA) ermöglicht, unabhängig ob diese IPv4 oder IPv6 sprechen, die notwendigen Informationen aus der Automatisierungsanlage zu erhalten, siehe Bild 6 und 7.

Dies macht es vor allem in einer Übergangszeit leicht, sich an die unterschiedlichen Netze anzupassen.

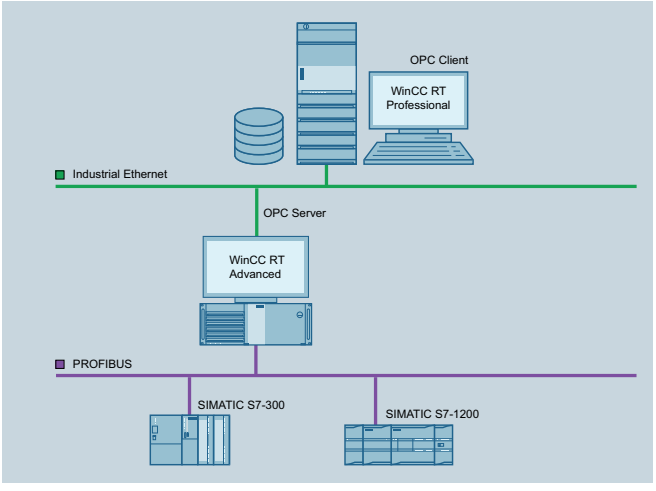


Bild 6: Übersicht OPC-Server

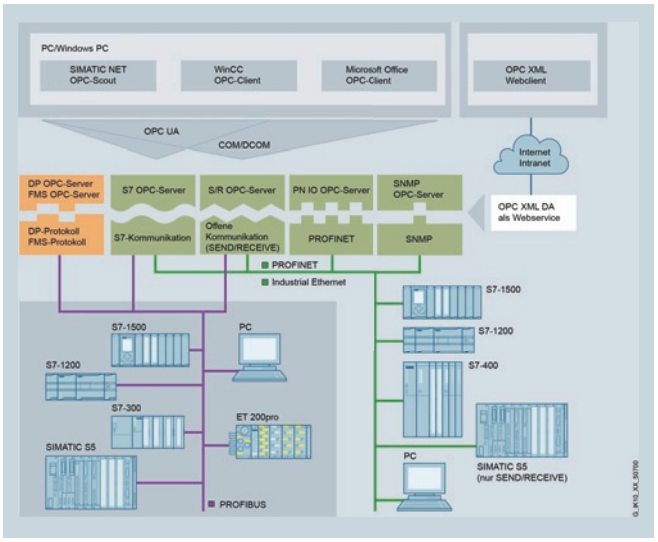


Bild 7: Blockschaltbild OPC Server

5.1 Beispiel OPC Client unter IPv6

Über ein Backbone Netzwerk wird in diesem Beispiel auf eine Anlage zugegriffen, welche noch IPv4 fähig ist oder andere Feldbussysteme wie z.B. PROFIBUS unterstützt, siehe Bild 8.

Der OPC-Client oder ein entsprechender OPC-Browser müssen mit der richtigen IPv6 Adresse konfiguriert werden.

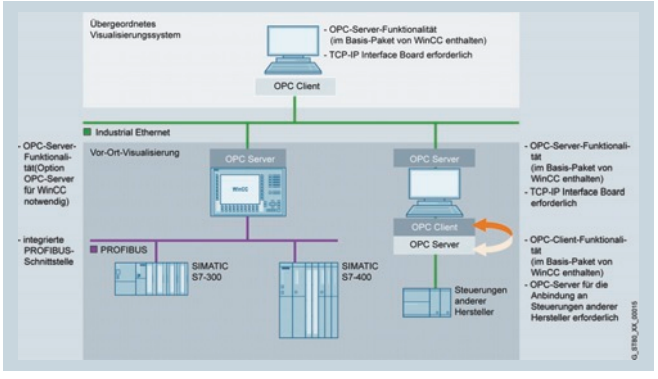


Bild 8: OPC Server, Zugriff auf PROFIBUS

IPv6 in der Automatisierungstechnik

Nach dem Zugriff auf den Server werden die vorhandenen Variablen angezeigt. Der Kunde merkt hier keinerlei Unterschiede, ob er sich über IPv4 oder IPv6 verbunden hat. Nur bei der Projektierung des Interfaces wird dies deutlich. Noch einfacher wird es, wenn man bei dem OPC-Server nur noch den Namen einer PC Station angibt. Hierzu sind jedoch entsprechende Industrial Network Services, wie z.B. DHCP und DNS notwendig.

6. Beispiel: SIMATIC S7-1500 mit CP 1543-1
Mit dem Kommunikationsprozessor CP 1543-1 wurde im Jahr 2013 erstmals von Siemens ein PLC-Produkt vorgestellt, welches für die Anbindung an den IPv6 Backbone entwickelt ist. Der CP 1543-1 bietet die Möglichkeit über die TCP Schnittstelle des PC mit IPv6 über die bekannten FETCH/WRITE Dienste auf Variablen der SIMATIC S7-1500 Station zuzugreifen. Damit ist es möglich, dass in einem Leitsystem die vorhandenen Kommunikationsmechanismen beibehalten werden oder sogar auf eine neue Transportschicht (in diesem Falle IPv6) aufgesetzt werden kann.

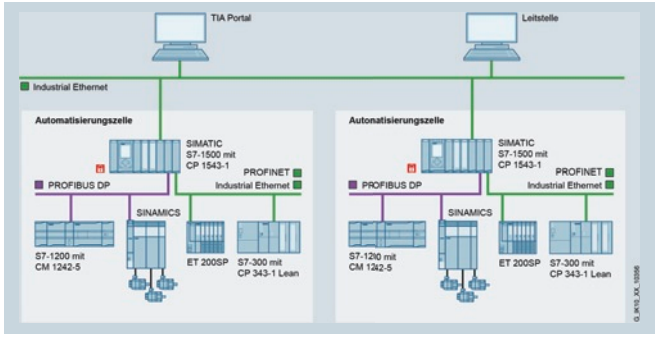


Bild 9: SIMATIC S7-1500, Darstellung FETCH/WRITE, FTP, Mail

Weitere Möglichkeiten zur Anbindung an eine neue IPv6-Infrastruktur werden mit FTP und Mail geboten.

6.1 Beispiel CP 1543-1 als FTP-Server
Für die Konfiguration eines IPv6 FTP-Servers sind bei dieser Baugruppe nur wenige Einstellungen über die Projektierungssoftware STEP 7 V12.0 notwendig:

- IPv6 Adresse für den CP 1543-1 festlegen (siehe Bild 10)
- Protokoll FTP oder FTPS aktivieren (siehe Bild 11)
- Benutzer mit Namen und Passwort anlegen (siehe Bild 12)
- Projektierungsdaten abspeichern und auf die Station übertragen

Bild 10: IPv6 Adresse automatisch beziehen

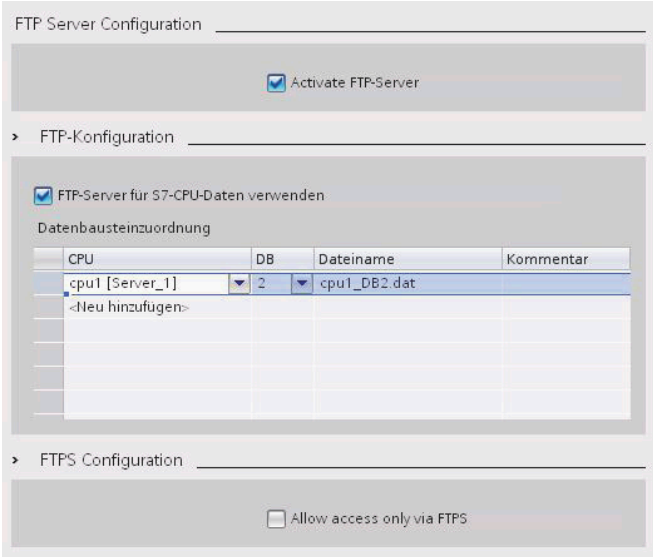


Bild 11: FTP-Protokoll aktivieren

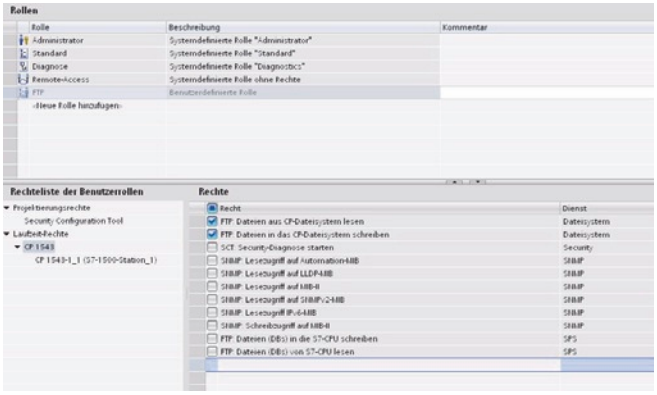


Bild 12: Benutzer anlegen und Zugriffsrechte festlegen

IPv6 in der Automatisierungstechnik

Damit ist die Projektierung in einer komfortablen Projektierungsoberfläche abgeschlossen und ein Zugriff auf Daten des PLC-Programms ist möglich.

Natürlich sind die Funktionen für IPv6 in dem Gesamtkonzept Security mit berücksichtigt. Der Anwender kann dabei festlegen, wie einzelne Benutzer oder Teilnehmer auf die Daten der Station zugreifen können.

Der Zugriff auf die Daten in einem Automatisierungsgerät ist mit frei verfügbaren Tools unter IPv6 möglich, siehe Bild 13.

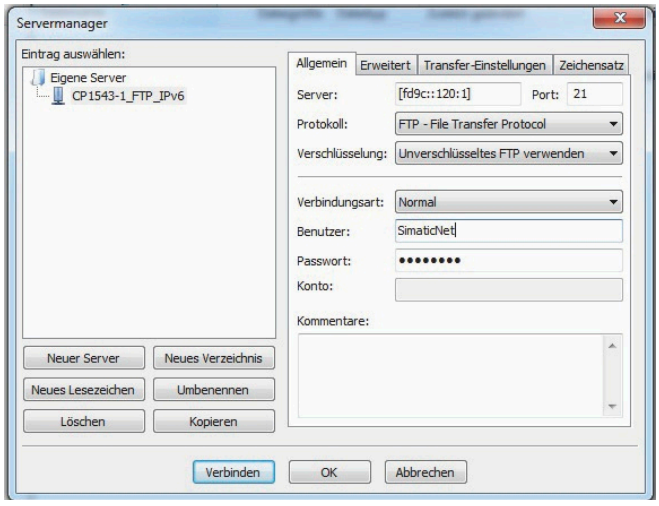


Bild 13: Datenzugriff mit allgemeinem FTP-Client Tool

7. Fazit und Aussicht

Die Bedeutung von IPv6 wird nicht zuletzt aufgrund der Verknappung von IPv4-Adressen zunehmen. Weltweit eindeutige IP-Adressen und die damit einhergehende Möglichkeit Anlagen und Produktionsstätten global nahtlos zu vernetzen, wird dazu führen, dass IPv6 in den nächsten Jahren nach und nach Einzug in IT/OT-Infrastrukturen halten wird.

Die Entscheidung zur Einführung von IPv6 in einem Netzwerk hat weitreichende Konsequenzen. Eine gewissenhafte Planung zur Umstellung, Zeit zum Testen und eine Strategie, wie lange man die bisherige IPv4-Infrastruktur noch parallel betreiben kann, sind erforderlich. Alle Erkenntnisse, die unter IPv4 gesammelt wurden, müssen bei einem Parallelbetrieb doppelt konfiguriert und gepflegt werden. Ein kompletter Umstieg auf IPv6 ist erst möglich, wenn sämtliche Teilnehmer durch IPv6 adressiert werden können und auch im World Wide Web die notwendige Infrastruktur geschaffen wurde.

Aus der IT-Welt kommende Übergangstechnologien, wie z.B. die Verwendung von IPv4 kompatiblen Adressen oder IPv4 mapped Adressen, die Verwendung von Tunneling Technologien wie IPv6-over-IPv4 beziehungsweise TEREDO erzeugen zusätzlichen Aufwand, reduzieren die Sicherheit und schränken teilweise die Funktionalität ein. Der Einsatz solcher Technologien sollte daher gründlich abgewogen werden. Speziell bei TEREDO, welcher als „die“ Lösung in der Vergangenheit gehandelt wurde, verzeichnet man in den letzten Jahren immer weiter abnehmenden Datenverkehr.

Um in Zukunft die Konnektivität zum Internet mit IPv6 sicherzustellen, ist die Einbindung der typischerweise auf IPv4 basierenden Automatisierungsnetze an die IPv6-Infrastruktur erforderlich.

Die Automatisierungsprodukte von Siemens mit IPv6-Unterstützung ermöglichen diese Backbone-Anbindung ohne auf die Verwendung von Übergangstechnologien angewiesen zu sein und gewährleisten so auch zukünftig die globale Vernetzung von Produktionsanlagen.

Abkürzungsverzeichnis

APNIC	Asia Pacific Network Information Centre, kurz APNIC ist die zuständige Regional Internet Registry (RIR) für die Region Asien und den Pazifik.	**PLC**	Programming Logical Controller, Überbegriff für frei programmierbare Steuerung.
DHCP	Dynamic Host Configuration Protocol,es ist mit BOOTP rückwärts kompatibel und in RFC 2131 definiert. Mit Hilfe von DHCP erfolgt die Netzwerkeinstellung z.B. eines Rechners (des DHCP-Clients) automatisch beim Start.	**RIR**	Regionalen Internet Registry, Non Profit Organisation für die Vergabe der Regionalen IP Adressen.
DHCPv6	DHCPv6 ist das Dynamic Host Configuration Protocol für IPv6, gemäß RFC 3315. Abweichend von DHCPv4 läuft bei v6 die Kommunikation über die UDP-Ports 546 (Client) und 547 (Server).	**RFC**	Request for Comments, zu Deutsch: Bitte um Kommentare, um technische Dokumente zu verbessern.
DNS	Domain Name Server: Server der die Auflösung einer symbolischen Internet Adresse in eine IP Adresse durchführt.	**SMPT**	Simple Mail Transfer Protocol, gemäß RFC 821, einfaches und weit verbreitetes E-Mail Transportprotokoll.
ERP	Enterprise Resource Planning, Anwendungssoftware zur Planung von Resourcen in einem Unternehmen.	**TEREDO**	Tunneling IPv6 over UDP through Network Address Translations (NATs) gemäß RFC 4380, Tunneltechnologie, welche es Teilnehmer hinter einem NAT-Router ermöglicht auf ein IPv6 Netzwerk zuzugreifen.
FTP	File Transfer Protocol, Definition nach RFC 959.		
IANA	Internet Assigned Numbers Authority, ist verantwortlich für die grundsätzliche Koordination im Internet, wie zum Beispiel die Vergabe von IP-Adressen oder Domain Namen.		
IPv4 Adresse	Numerische eindeutige Adresse für jeden IPv4-Teilnehmer im Internet, z.B. 120.0.1.2		
IPv6 Adresse	Hexadezimale eindeutige Adresse für jeden Teilnehmer im Internet, z.B. 2001:000A:000B:000C:0000:0000:ABCD:0001		
LTE	Long Term Evolution, Bezeichnung für den Mobilfunkstandard der dritten Generation.		
NAT	Network Address Translation, Methode um IPv4 Adressen in Netzwerken umzuschreiben.		
OPC UA	OPC Unified Architecture, industrielles M2M-Kommunikationsprotokoll, welches die Maschinendaten auch semantisch beschreibt.		
OT	Operational Technology, Software und/oder Hardware, welche direkt in die Prozesse im Unternehmen eingreift		
PAT	Port and Address Translation, dabei werden im Gegensatz zu NAT nicht nur die IP-Adressen, sondern auch die Port-Nummern umgeschrieben. PAT wird eingesetzt, wenn mehrere private IP-Adressen aus einem LAN zu einer öffentlichen IP-Adresse übersetzt werden sollen.		

Herausgeber
Siemens

Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Germany

PDF
White Paper
6ZB5530-0DH01-0BA0
BR 0619 10 De

Security-Hinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen.

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen einen Bestandteil eines solchen Konzepts.

Die Kunden sind dafür verantwortlich, unbefugten Zugriff auf ihre Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Diese Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und nur wenn entsprechende Schutzmaßnahmen (z.B. Firewalls und/oder Netzwerksegmentierung) ergriffen wurden.

Weiterführende Informationen zu möglichen Schutzmaßnahmen im Bereich Industrial Security finden Sie unter **https://www.siemens.com/industrialsecurity.**

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Produkt-Updates anzuwenden, sobald sie zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter **https://www.siemens.com/industrialsecurity.**