SIEMENS

Industrial Ethernet

IPv6 in automation technology

White Paper

Edition 06/2019

siemens.com/industrial-ethernet

Content

IPv6 in automation technology

1. Basics and use of IPv6

The significance of the Internet Protocol Version 6 (IPv6) will increase, not least due to the increasing shortage of IPv4 addresses. Worldwide unique IP addresses and the associated opportunity to seamlessly network systems and production facilities globally will lead to IPv6 slowly but surely moving into IT and OT infrastructures in the next few years. In addition to technical basics, the examples beginning in Chapter 5 will also provide users with specific help in deploying the new technology.

2. IPv6 for automation technology

The introduction of IPv6 in automation technology is more than just a simple quadrupling of the existing 32-bit IPv4 address to a 128-bit address to increase the number of IP addresses. The massively expanded address space also allows us to do without the previously introduced address conversions due to limited IPv4 address space. In future, this will allow problem-free direct communication between end systems without the complicated and errorprone address acrobatics resulting from network address translation (NAT). There will only be pure "end-to-end" communication in the future. Limiting technologies such as NAT/PAT will no longer be required.

What are the user benefits that will be achieved with the introduction of the new IPv6 technology?

- Consistent diagnosis from the ERP level to the management level all the way down to the field level
- Hierarchical setup of network structures
- Optimized routing

New IT technologies will be based exclusively on IPv6, while simultaneously a coexistence between IPv4 and IPv6 must be considered for a long time. Today, there is no longer a question as to whether there will be a transition from IPv4 to IPv6, but when!

In future, IPv6 will be predominant on the ERP level, because new functions within the software will be based directly on IPv6 services.

Because of the increasingly close mesh between automation and enterprise IT, IPv6-based communication services are of growing importance for integrated diagnostics, including for programmable controllers.

3. Basics of IPv6

3.1 Turning point/initial situation

On February 1, 2011, the time had come: The Internet Assigned Numbers Authority (IANA) issued the last free address block to the Asia-Pacific Network Information Center (APNIC). With this move, there were no more IPv4 addresses available to distribute to the five Regional Internet Registries (RIR). The RIRs can only pass on the remaining IPv4 addresses they hold to their customers.

For users of the Internet Protocol IPv4, this meant the switch to the IPv6, defined 15 years earlier, had begun. Operating systems such as Windows or Linux had supported this for years.

In the short term, users will still be given IPv4 addresses from the Regional Internet Registry pool, but in the midterm, worldwide availability using these will not be ensured. The only way out of this misery is the use of globally unique IPv6 addresses so that "end-to-end" communication can once again be ensured.

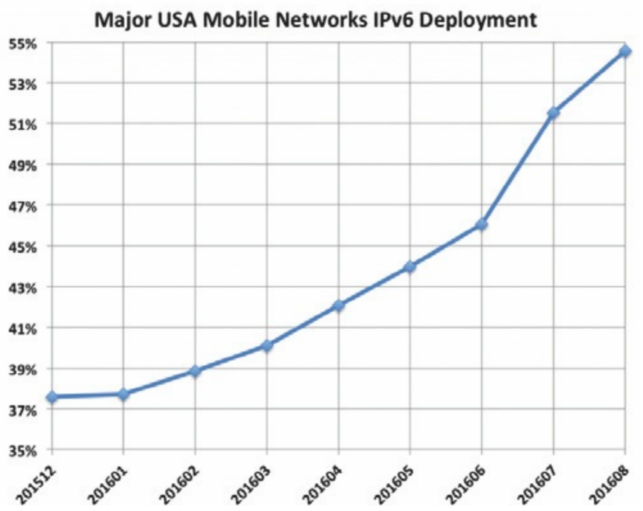


Fig. 1: Increase in IPv6 data traffic with the large mobile radio providers
Source: **https://www.worldipv6launch.org/major-mobile-us-networks-pass-50-ipv6-threshold/**

IPv6 in automation technology

For public networks, one possible analysis method is to evaluate the information from the BGP (Border Gateway Protocol) table of the routers and to bring these into proportion, see Fig. 2.

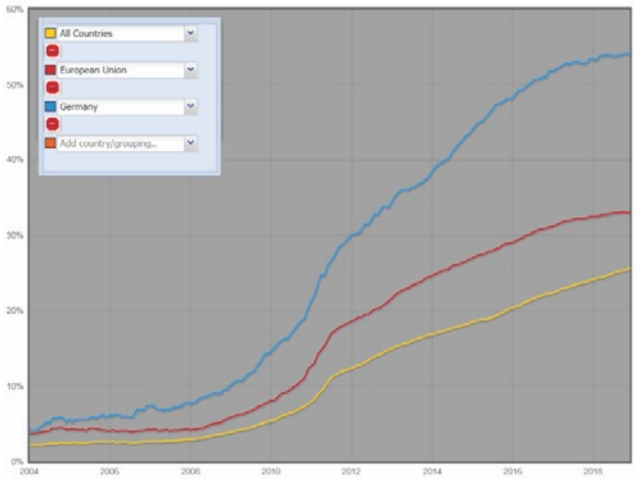


Fig. 2: Increase in IPv6 routes, worldwide (yellow), European Union (red) and Germany (blue)
Source: **http://v6asns.ripe.net/v/6?s=_ALL;s=_RIR_RIPE_NCC**

All the worldwide evaluations show a significant increase in IPv6 communication over the last four years. In some countries, such as Brazil, telecommunications via LTE is now only possible with IPv6 "Support". Devices just with IPv4 communication are no longer permitted.

3.2 Standardization

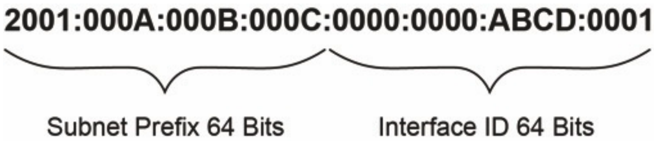
The standardization, which began in 1998 with RFC 2460 as the official successor to the IPv4 protocol, is today in a stable condition. Many extensions such as the coexistence of IPv4/IPv6, DHCPv6, neighbor discovery, and many more have since been described in the various RFCs. The following RFCs are recommended for more in-depth information:

- 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 IPv6 address structure v6

In contrast to IPv4, the IPv6 addresses are written in 8 x 16-bit fields of four hexadecimal numbers each. These are separated from each other with a colon. There is always a 64-bit subnet prefix and a 64-bit interface ID.

An example of this would be a global IPv6 address in the following notation:



Mathematically, 340,282,366,920,938,463,463,374,607,431, 768,211,456 addresses are possible. To more or less illustrate this unimaginably large number, every proton in the universe could have its own IP address. Or, in other words, every square meter of the earth's surface could have "merely" 6.5 x 10^{23} addresses.

Clarification of the address space:

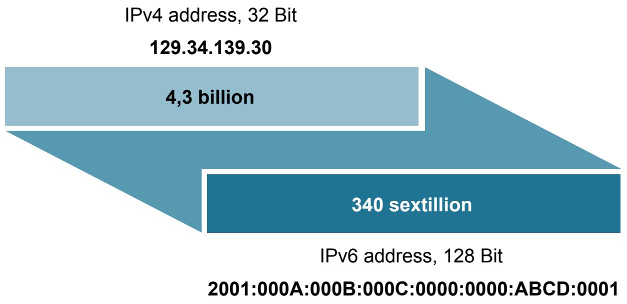


Figure 3: Size of the IP address space

Since enough unambiguous addresses are available to allow unambiguous addressing and thus a direct connection between nodes, network address translation (NAT) and port address translation (PAT) are no longer necessary.

IPv6 in automation technology

3.2.2 Many addresses at one interface

With IPv6 addressing, every network interface is given at least one address; in most cases, however, several addresses. Alongside the link-local address (LLA, always formed automatically for each interface), which is important for issuing addresses, this can also include a unique local address (ULA) or even a global address (GA).

Note:
The LLA, which is automatically generated by each device and is always unambiguous, allows all devices on the local subnet to be reached via IPv6. The devices are thus always available and diagnosable.

Manual configuration or any other setting of the IPv6 address is not necessary.

Further information can also be found in the RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture.

3.2.3 IPv6 address assignment

One of the most important new features of IPv6 is automatic address assignment. Using the auto-configuration, any IP node can create a unique link-local address itself without requiring manual configuration or a DHCP server.

For additional use of router discovery:

- Further IPv6 addresses
- Router addresses
- Further configuration parameters

are provided to the node. It is hoped that this will significantly reduce the effort required for administration of networks, see Fig. 4.

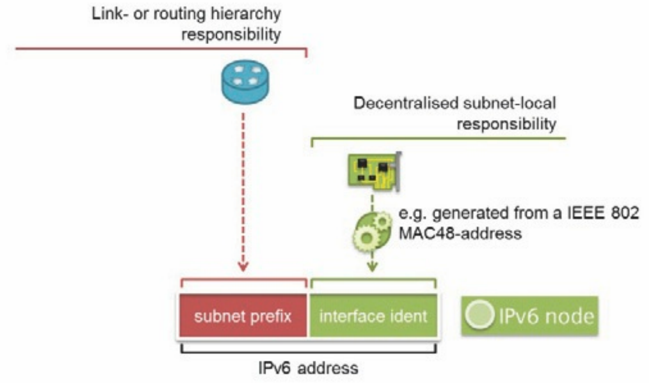

Link- or routing hierarchy responsibility
Decentralised subnet-local responsibility
e.g. generated from a IEEE 802 MAC48-address
subnet prefix
interface ident
IPv6 node
IPv6 address

Fig. 4: IPv6 address structure

3.2.4 Dual stack

The term dual stack generally refers to a complete duplication of the IPv4 and IPv6 stacks across all levels in the protocol stack, from the application layer to the network layer. The dual-stack approach ensures that the further-developed components can always interoperate via IPv4 using only IPv4 components. In automation technology, it ensures compatibility with existing system components.

3.2.5 Significant IPv4/IPv6 differences

Content	IPv4	IPv6
Released	1981 (RFC 791)	1998 (RFC 2460)
Available address space	32 Bit, 4,29x10^9 adresses	128 Bit, 3,4x10^{38} adresses
Address format	Dezimal: 192.168.1.1	Hexadezimal: 2a00:ad80::0123
Loopback address	127.0.0.1	1
IPsec header	Optional	Always available
Fragmentation	Host and router	Only the communication endpoint
Checksum in the header	yes	no
Options in the header	yes	no
Link-layer address resolution	ARP (broadcast)	Multicast neighbor discovery messages
Router discovery	optional	Mandatory
IP configuration	Manual, DHCP	Automatic, DHCPv6, manual

Fig. 5: Table of IPv4/IPv6 differences

4. Investment protection

The introduction of IPv6 is primarily driven by the fact that the address range of the global IP network (Internet) has been exhausted. An expanded address space was defined already many years ago with IPv6 to address this shortage.

Therefore, the implementation of the new addressing primarily affects the backbone area of a company and will later migrate gradually via the IT infrastructure to the automation level.

This transition will take a long time and will also make it necessary for the two procedures to exist parallel to each other.

IPv6 in automation technology

Additional IPv6 support for new devices provides trouble-free global accessibility without affecting the existing communication links.

The simultaneous use of IPv4 and IPv6 communication (see Chapter 3.2.4, dual stack) requires above all, from the network perspective, support in the Layer 3 devices (routing). In principle, existing layer 2 devices (switches) allow both IPv4 and IPv6 communication; to fully support IPv6, however, adjustments on this level are also necessary.

This duality means there is stock protection for existing systems and retrofitting or upgrading is only required in exceptional cases.

5. Example: OPC server

It is already possible to communicate over IPv6 today by using the OPC server by Siemens. The OPC server takes on the role of a proxy here, offering convenient access to the automation data via IPv4 and IPv6. This also allows OPC clients (HMI/SCADA) to obtain the necessary information from the automation system, regardless of whether they speak IPv4 or IPv6, see Fig. 6 and 7.

This makes it easy to adapt to the different networks, especially during a transitional period.

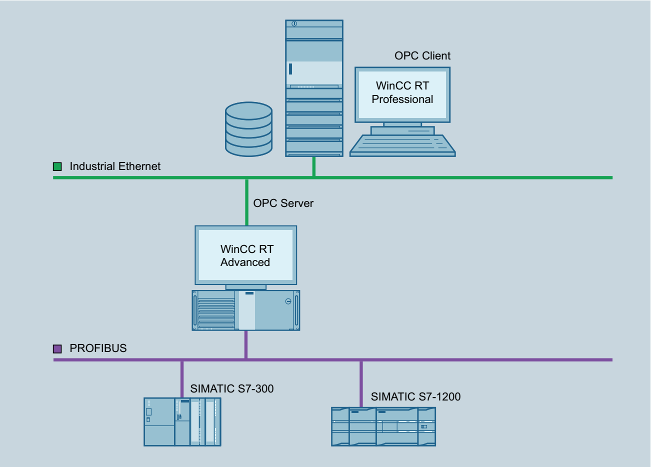


Fig. 6: Overview of OPC server

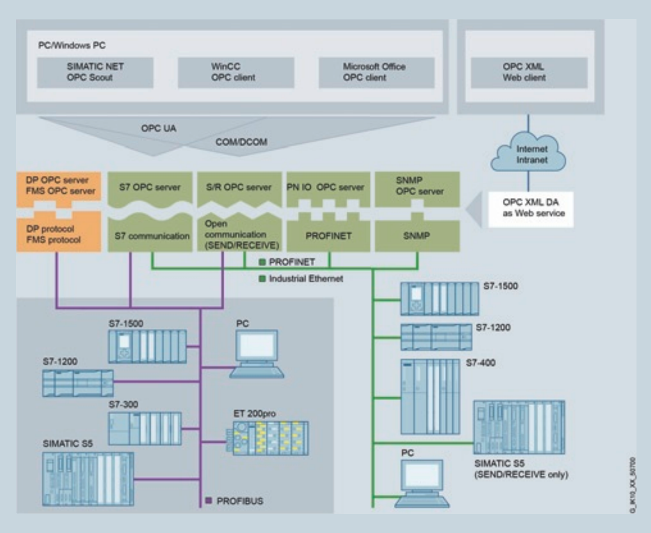


Fig. 7: OPC server block diagram

5.1 Example of OPC client under IPv6

In this example, a system that is still IPv4-capable or supports other fieldbus systems such as PROFIBUS is accessed via a backbone network, see Fig. 8.

The OPC client or a corresponding OPC browser must be configured with the correct IPv6 address.

After access to the server, the existing variables are shown. The customer notices no difference here whether he has connected via IPv4 or IPv6. This only becomes clear when configuring the interface. It is even easier if you only specify the name of a PC station with the OPC server.

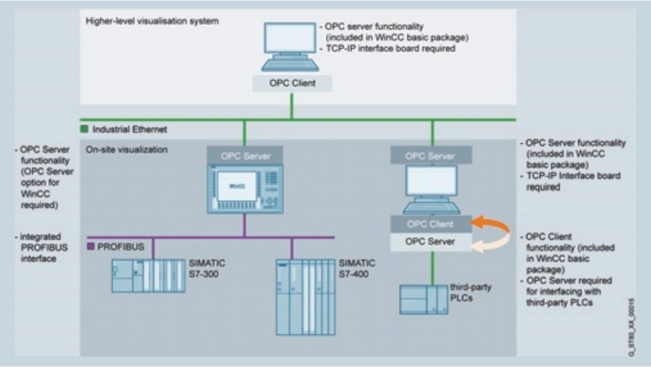

Higher-level visualisation system
- OPC server functionality (included in WinCC basic package)
- TCP-IP interface board required
OPC Client
Industrial Ethernet
- OPC Server functionality (OPC Server option for WinCC required)
- integrated PROFIBUS interface
On-site visualization
OPC Server
WinCC
OPC Server
OPC Client
OPC Server
- OPC Server functionality (included in WinCC basic package)
- TCP-IP Interface board required
- OPC Client functionality (included in WinCC basic package)
- OPC Server required for interfacing with third-party PLCs
PROFIBUS
SIMATIC S7-300
SIMATIC S7-400
third-party PLCs
G_ST80_XX_00015

Fig. 8: OPC server, access to PROFIBUS

IPv6 in automation technology

6. Example: SIMATIC S7-1500 with CP 1543-1

The communications processor CP 1543-1 is the first Siemens PLC product designed to connect to the IPv6 backbone. The CP 1543-1 offers the ability to access variables of SIMATIC S7-1500 station using the familiar FETCH/WRITE services via the TCP port of the PC with IPv6. It is thus possible that the existing communication mechanisms can be retained in a control system or even placed on a new transport layer (in this case IPv6).

Other ways to connect to a new IPv6 infrastructure are by FTP and e-mail.

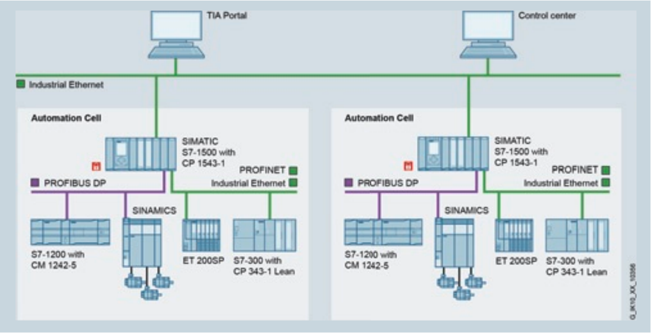


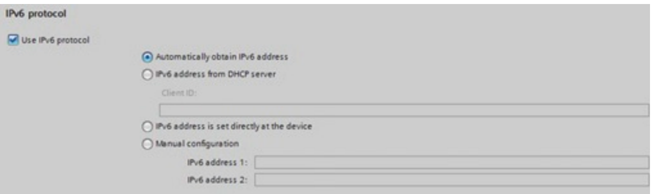
Fig. 9: SIMATIC S7-1500, representation of FETCH/WRITE, FTP, e-mail

6.1 Example: CP 1543-1 as FTP server

To configure an IPv6 FTP server, for this module only a few settings are necessary using the configuration software STEP 7 V12.0:

- Define IPv6 address for the CP 1543-1 (see Fig. 10)
- Activate FTP or FTPS protocol (see Fig. 11)
- Create user with name and password (see Fig. 12)
- Save configuration data and transfer it to the station

The configuration is thus completed in a user-friendly configuration interface and access to data of the PLC program is possible.

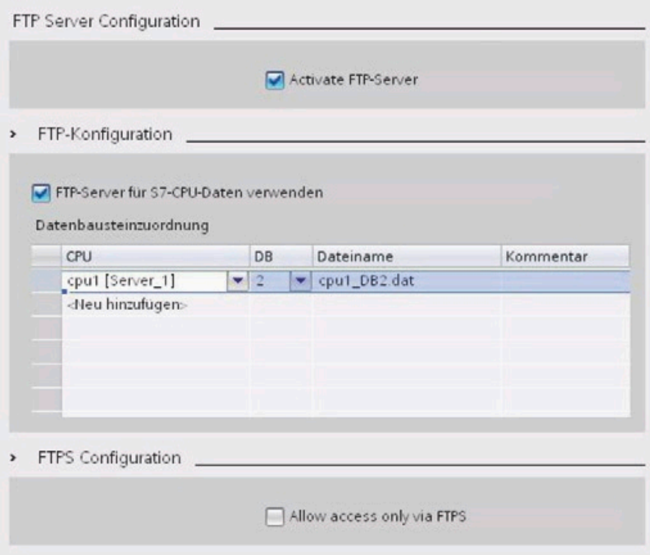


IPv6 protocol

☑ Use IPv6 protocol

● Automatically obtain IPv6 address
○ IPv6 address from DHCP server
Client ID:
○ IPv6 address is set directly at the device
○ Manual configuration
IPv6 address 1:
IPv6 address 2:

Fig. 10: Obtaining an IPv6 address automatically



FTP Server Configuration

☑ Activate FTP-Server

› FTP-Konfiguration

☑ FTP-Server für S7-CPU-Daten verwenden

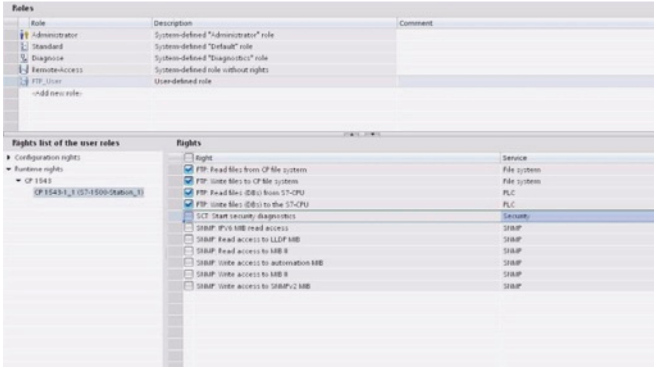
Datenbausteinzuordnung

CPU	DB	Dateiname	Kommentar
cpu1 [Server_1]	2	cpu1_DB2.dat	
<Neu hinzufügen>			

› FTPS Configuration

☐ Allow access only via FTPS

Fig. 11: Activation of the FTP protocol



Roles

Role	Description	Comment
Administrator	System-defined "Administrator" role	
Standard	System-defined "Default" role	
Diagnose	System-defined "Diagnostics" role	
Remote-Access	System-defined role without rights	
FTP_User	User-defined role	
<Add new role>		

Rights list of the user roles

- ▸ Configuration rights
- ▾ Runtime rights
  - ▾ CP 1543
    - CP 1543-1_1 (S7-1500-Station_1)

Rights

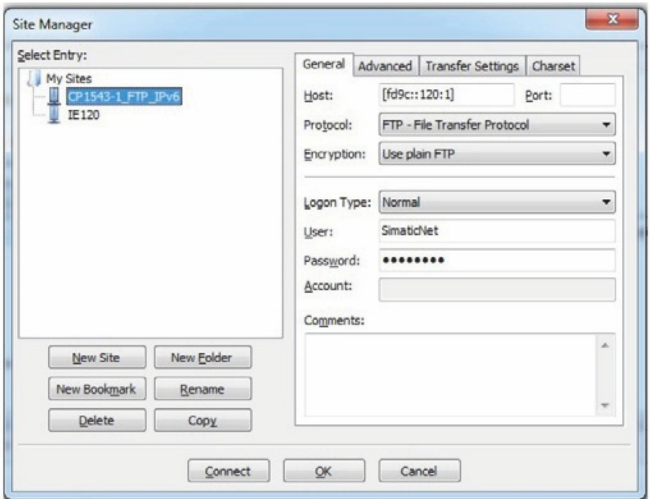
☐ Right	Service
☑ FTP: Read files from CP file system	File system
☑ FTP: Write files to CP file system	File system
☑ FTP: Read files (DBs) from S7-CPU	PLC
☑ FTP: Write files (DBs) to the S7-CPU	PLC
☐ SCT: Start security diagnostics	Security
☐ SNMP: IPV6 MIB read access	SNMP
☐ SNMP: Read access to LLDP MIB	SNMP
☐ SNMP: Read access to MIB II	SNMP
☐ SNMP: Write access to automation MIB	SNMP
☐ SNMP: Write access to MIB II	SNMP
☐ SNMP: Write access to SNMPv2 MIB	SNMP

Fig. 12: Creating users and setting access rights

IPv6 in automation technology

Of course, the functions for IPv6 in the overall security concept are also considered. The user can specify how individual users or nodes can access the data of the station.

Access to the data in a programmable controller is possible with freely available tools under IPv6, see Fig. 13.



My Sites
- CP1543-1_FTP_IPv6
- IE120

Host: [fd9c::120:1]
Port:
Protocol: FTP - File Transfer Protocol
Encryption: Use plain FTP
Logon Type: Normal
User: SimaticNet
Password: ••••••••
Account:

Fig. 13: Data access with general FTP client tool

7. Conclusion and outlook

The significance of IPv6 will increase not least due to the increasing shortage of IPv4 addresses. Worldwide unique IP addresses and the associated opportunity to seamlessly network systems and production facilities globally will lead to IPv6 slowly but surely moving into IT/OT infrastructure in the next few years.

The decision to introduce IPv6 in a network has far-reaching consequences. Careful planning for conversion, time for testing, and a strategy for how long the existing IPv4 infrastructure can be run in parallel are required. All findings gathered under IPv4 must be configured and maintained twice in parallel operation. A complete switch to IPv6 is only possible if all nodes can be addressed by IPv6 and the necessary infrastructure has been created on the World Wide Web.

Transitional technologies from the IT world such as the use of IPv4-compatible addresses or IPv4-mapped address, and the use of tunneling technologies such as IPv6-over-IPv4 or TEREDO generate additional overhead, reduce security, and partially restrict functionality. The use of such technologies should therefore be weighed up carefully.

To ensure connectivity to the Internet in future with IPv6, the integration of automation networks typically based on IPv4 in the IPv6 infrastructure is necessary. The first automation products with IPv6 support from Siemens allow this backbone connectivity without requiring the use of transition technologies, thus ensuring the global networking of production plants in the future as well.

Abbreviations

APNIC	The Asia Pacific Network Information Center (APNIC) is the regional Internet registry (RIR) responsible for the Asia/Pacific region.	**PLC**	Programmable Logic Controller, an umbrella term for a freely programmable control.
DHCP	The Dynamic Host Configuration Protocol is backward compatible with BOOTP and defined in RFC 2131. Using DHCP, the network setting of, for example, a computer (the DHCP client) is performed automatically at startup.	**RIR**	Regional Internet Registry, non-profit organization for the assignment of regional IP addresses.
DHCPv6	DHCPv6 is the Dynamic Host Configuration Protocol for IPv6 in accordance with RFC 3315. Contrary to DHCPv4, in v6 communication runs via the UDP ports 546 (client) and 547 (server).	**RFC**	Request for comments to improve technical documents.
DNS	Domain Name Server: Server that resolves a symbolic Internet address as an IP address.	**SMPT**	Simple Mail Transfer Protocol, as per RFC 821, a simple and widely used e-mail transport protocol.
ERP	Enterprise Resource Planning, application software for planning resources in a company.	**TEREDO**	Tunneling IPv6 over UDP through Network Address Translations (NATs) as per RFC 4380, tunnel technology that allows nodes behind a NAT router to access an IPv6 network.
FTP	File Transfer Protocol, definition according to RFC 959.		
IANA	Internet Assigned Numbers Authority, responsible for the basic coordination in the Internet, such as the allocation of IP addresses and domain names.		
IPv4 Adresse	Unique numerical address for each IPv4 node on the Internet, e.g. 120.0.1.2		
IPv6 Adresse	Unique hexadecimal address for each node on the Internet, e.g. 2001:000A:000B:000C:0000:0000:ABCD:0001		
LTE	Long Term Evolution, term for the third-generation mobile radio standard.		
NAT	Network Address Translation, a method to rewrite IPv4 addresses in networks.		
OPC UA	OPC Unified Architecture, industrial M2M communications protocol that also describes the machine data semantically.		
OT	Operational technology, software and/or hardware that directly influences company processes		
PAT	OPC Unified Architecture, industrial M2M communications protocol that also describes the machine data semantically. Port and Address Translation, where in contrast to NAT, not only the IP addresses, but also the port numbers are rewritten. PAT is used if multiple private IP addresses from a LAN must be translated into a public IP address.		

Published by
Siemens

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

PDF
White Paper
6ZB5530-0HD02-0BA0
BR 0619 10 En
© Siemens 2019

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations may be trademarks or product names of Siemens AG or supplier companies whose use by third parties for their own purposes could violate the rights of the owners.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit
https://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under
https://www.siemens.com/industrialsecurity.

siemens.com/industrial-ethernet