



以太网的S7通信 (集成PN接口的CPU和CP)

- 通信资源
- 数据交换

以太网接口的CPU和CP

- 伴随Profinet技术的发展，西门子对于CPU进行了升级，CPU开始集成一个Profinet接口，例如CPU315-2PN/DP, CPU414-3PN/DP等。不久将推出具有双端口交换机的Profinet接口的CPU，而且尺寸保持不变。
- 伴随以太网技术的发展，西门子以太网通讯模块对原来的CP343-1/CP443-1模板进行了升级，现在目前最新的CP343-1(343-1GX30-0XE0)和CP443-1(443-1GX20-0XE0)，除了集成Profinet接口，还扩展了一个1G以太网接口，用于连接到千兆以太网中与监控设备通讯。
- 这里主要涉及具有集成PN接口的CPU和CP，对于PB接口的设备CPU和CP的S7相关的通讯以及MPI的S7相关通讯，请参考网上课堂下载中心 <http://www.ad.siemens.com.cn/download/>。

以太网接口的**CPU**和**CP**的通讯服务

CPU的PN接口所支持的通讯服务包括：

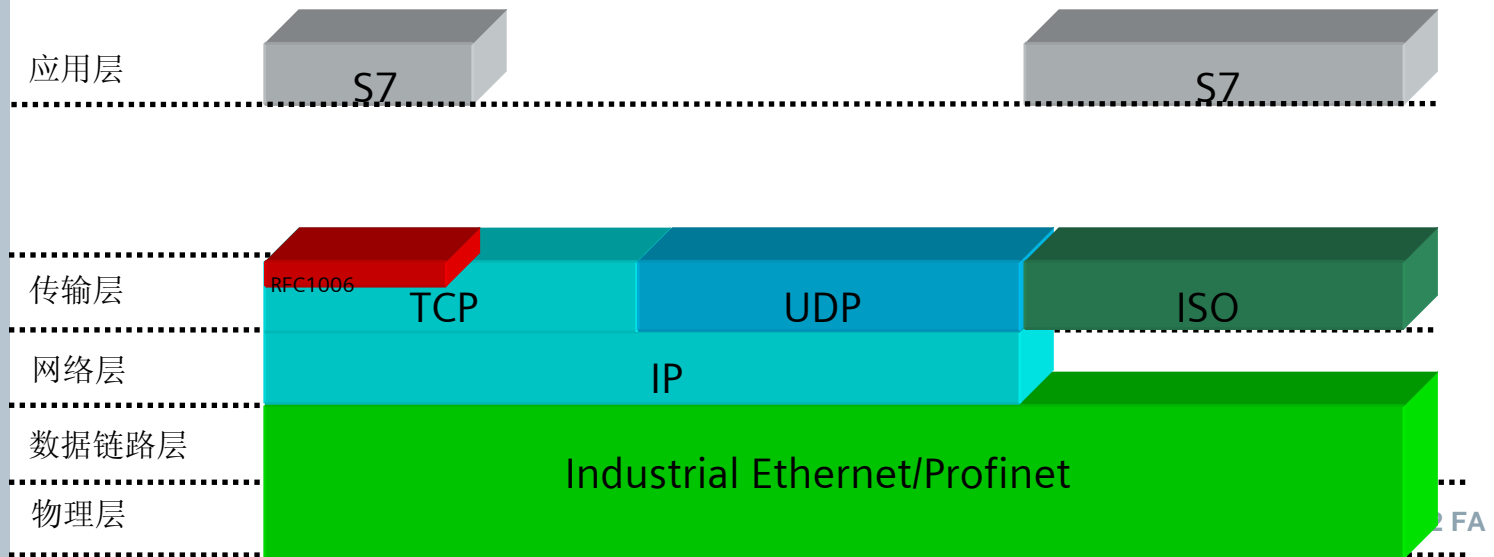
- PG通讯
- OP通讯
- S7通讯
- PN IO通讯
- PN CBA通讯
- Web server
- Open IE
- 路由

CP的PN接口所支持的通讯服务包括：

- PG通讯
- OP通讯
- S7通讯
- PN IO通讯
- PN CBA通讯
- Web server
- S5兼容的通讯

以太网的S7协议

- S7协议是西门子专有协议，广泛用于各种通讯服务，例如：PG通讯，OP通讯，S7基本通讯，S7通讯，路由等。
- S7协议独立于西门子各种通讯总线，可以在MPI，PROFIBUS，Ethernet，PROFINET上运行。
- S7协议是由多种应用层协议组成的，或者说S7协议是一个由多种协议的集合协议。
- S7协议在以太网上的底层协议根据应用不同使用ISO, ISO on TCP。



通信资源

- 通信资源就是通信双方为了执行通信服务而进行的连接资源和通信任务资源的分配。通信双方的数据交换需要通信资源，由其中的连接资源和通讯任务资源两个参数决定。
- 当超过连接资源，新加入的通讯双方无法进行通讯。例如CPU319-3PN/DP具有16个S7连接资源，当通过NetPro组态S7 Connection通讯连接设置为16个后，就无法再加入其它的通讯Partner与该CPU进行通讯。
- 当超过通讯任务资源，其它连接资源的通讯双方无法进行通讯。例如CPU319-3PN/DP组态了16个S7 Connection通讯，其中一个连接使用了32个通讯任务，那么CPU319就无法与剩余的15个连接Partner进行通讯。

通信资源示例

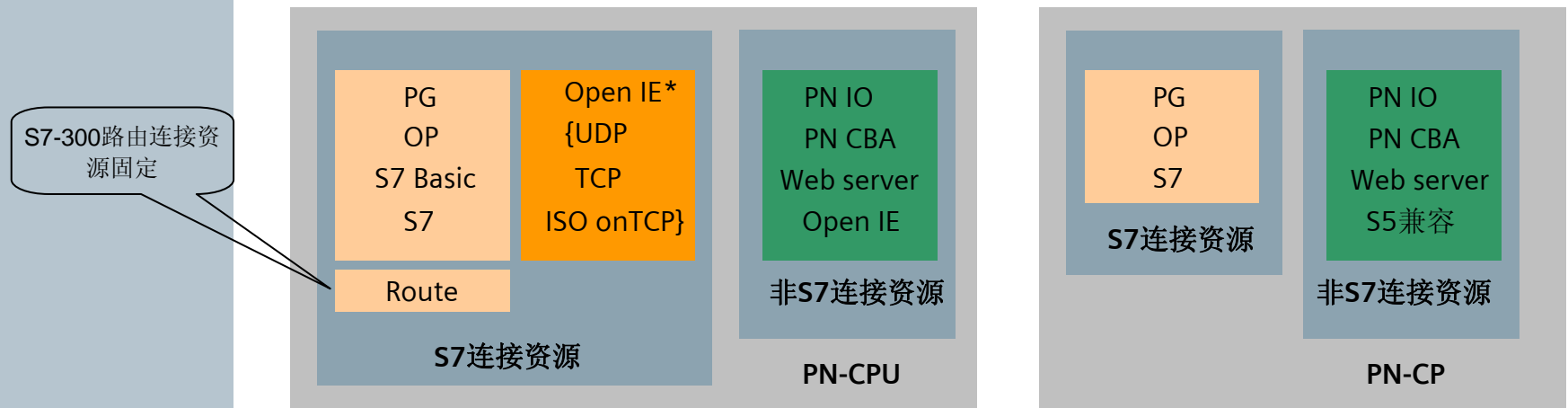
- S7-300和S7-400的PLC中定义，凡是通讯都需要通信资源。例如CP343-1(343-1GX30-0XE0)手册中提到PROFINET IO的性能参数：

Characteristic	Explanation / values
Number of possible PROFINET IO devices	128, including a maximum of 32 IRT devices If data is stored on the CPU, the number of operable PROFINET IO devices may be < 128. This depends on the free configuration memory available on the CPU type you are using.
Size the input area over all PROFINET IO devices *)	4096 bytes max.
Size the output area over all PROFINET IO devices	4096 bytes max.

- 其中连接资源：PROFINET IO RT通讯的连接数量是128个。而通讯任务：PROFINET IO设备的输入输出分别为4096个字节。这两类参数表征了连接资源。

连接资源

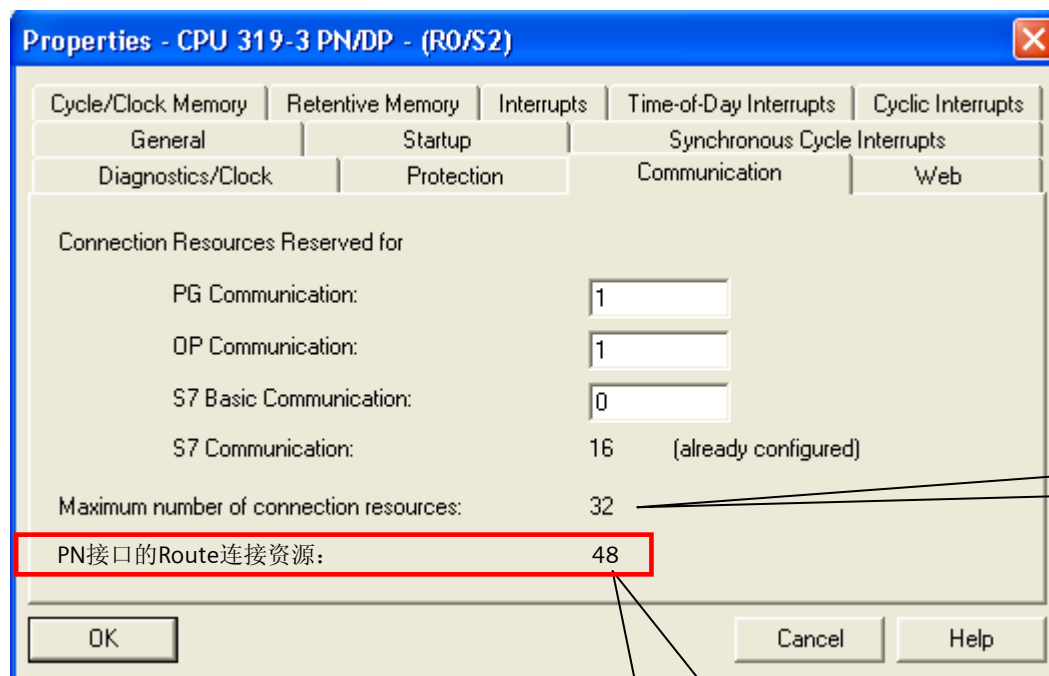
- 集成PN接口的CPU/CP提供相应的连接资源满足其各种各样的通讯服务。主要分为两类连接资源，一类是S7连接资源；另一类是非S7连接资源。
- S7连接资源是CPU/CP使用S7协议下的相关的通信服务而进行的连接数量和逻辑资源的分配。第一类的S7连接资源有着广义上的意义，除了与S7协议相关的服务，还可以给其它通讯服务，例如Open IE(S7-400)提供逻辑资源。



*S7-400PN的CPU做Open IE会占用S7连接资源

S7连接资源- S7-300CPU

- 在S7-300的CPU属性中可以分配S7连接资源给相应的S7通信服务。而S7-300的CPU中路由连接资源是独立提供的，并不占用CPU所提供的其它相应S7的通信服务。例如：根据CPU319-3PN/DP的技术数据，PN接口的路由资源数最大为48。其它S7相应的连接资源为32个，这些连接资源用于PG/OP/S7 Basic/S7通讯服务。



32个S7连接资源分配给PG/OP/S7 basic/S7

S7-300路由连接资源固定

S7连接资源- S7-400CPU

- 在S7-400的CPU属性中无法分配相应的S7连接资源。相应的S7通讯服务共同占用CPU所提供的所有的S7连接资源。只能通过CPU在线的方式查看CPU的S7连接资源的占用状态。例如：CPU416-3PN/DP

CPU所能提供的最大的S7连接资源数量

Other Communication: 包括路由资源*, Open IE连接资源, 等等

Connection Resources			
Maximum number:	64	Not used:	61
	Reserved	Occupied	
PG communication:	1	1	
OP communication:	1	0	
S7 communication	0	0	
Other communication:	--	2	
Open communication via Industrial Ethernet			
Connection resources in use:		2	

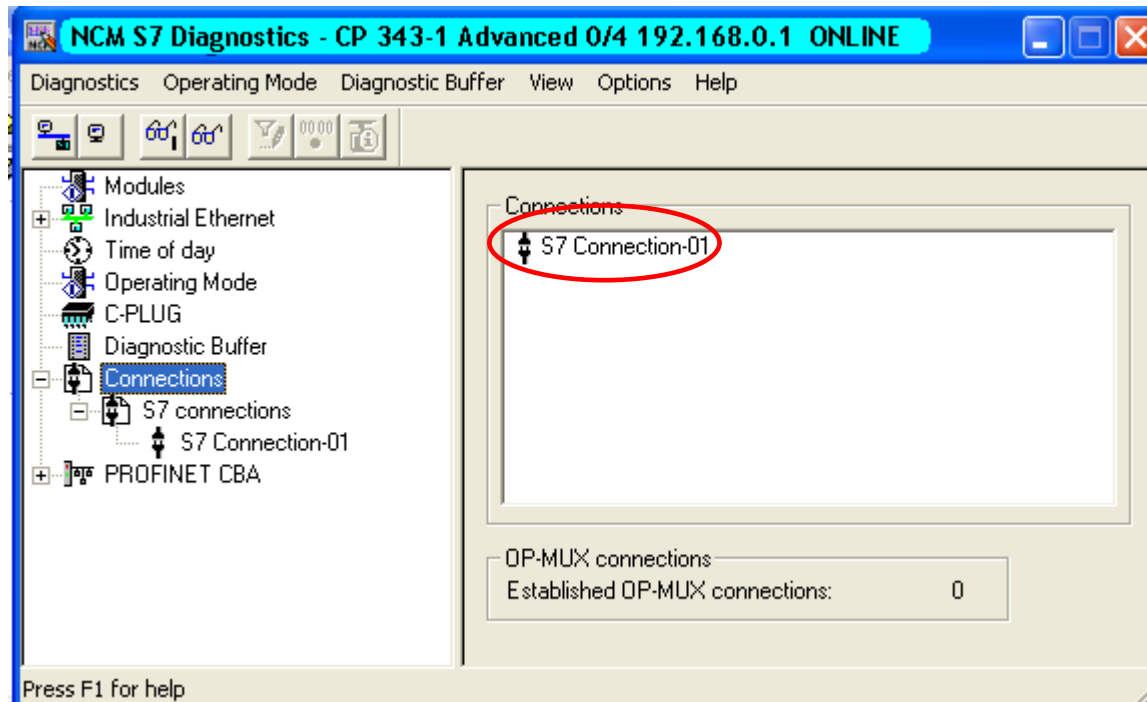
Open IE会占用CPU的S7连接资源

*S7-400PLC每一个路由由会占用2个S7连接资源 © CS CS2 FA

S7连接资源-S7-300CP

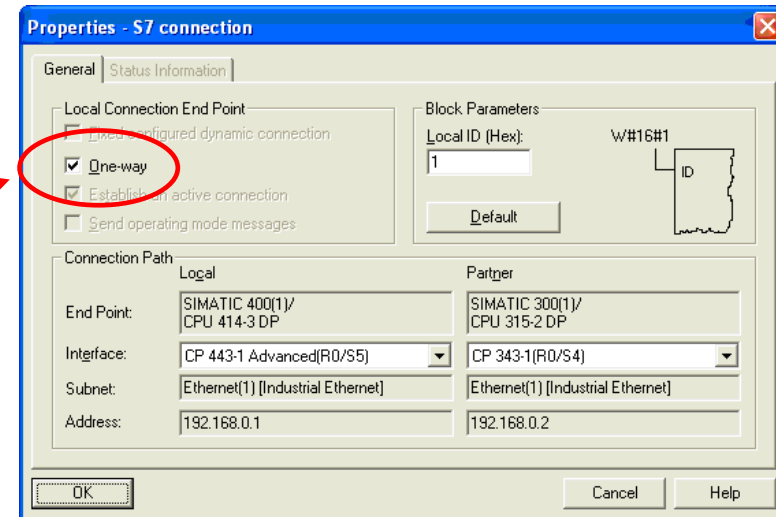
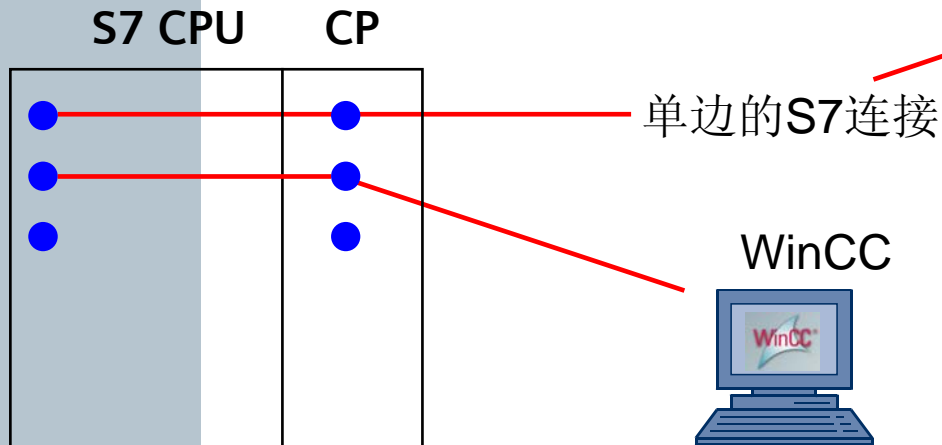
- S7-300CP卡无法按照通讯服务来分配相应的S7连接资源。相应的S7通讯服务共同占用CP所提供的S7连接资源。只能通过CP在线的方式查看CP的S7连接资源的占用状态。下图为CP343-1GX30的在线

Connection status	Local ID	Partner ID	Partner	Type	Active connection partner	Subnet
▶ Set up	1	1	SIMATIC 400(1) / CPU 416F-3 PN/DP	S7 connection	Yes	Ethernet(1) [IE]



S7-300CP多路复用

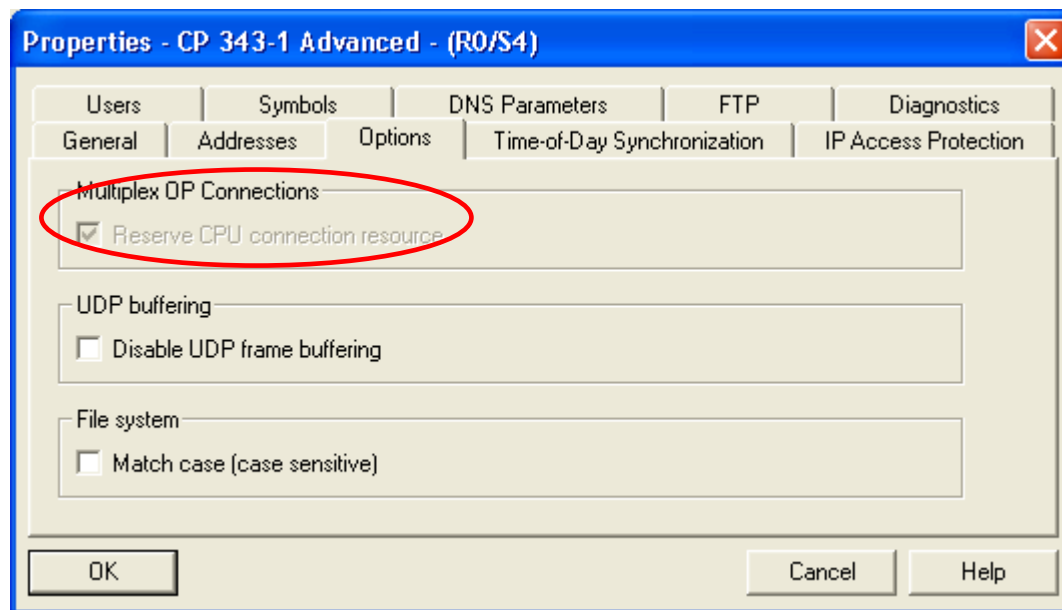
- S7连接通讯的终点不是CP，而是CPU，所以虽然在CP板也存在S7连接资源，但是最终会占用CPU的连接资源，这就是为什么必须需要相应地改变CPU通信设置的原因（S7-300PLC的S7连接资源数量远小于S7-400PLC）。
- CPU为每个单边的S7连接和WinCC预留单独的连接资源。



● S7连接资源

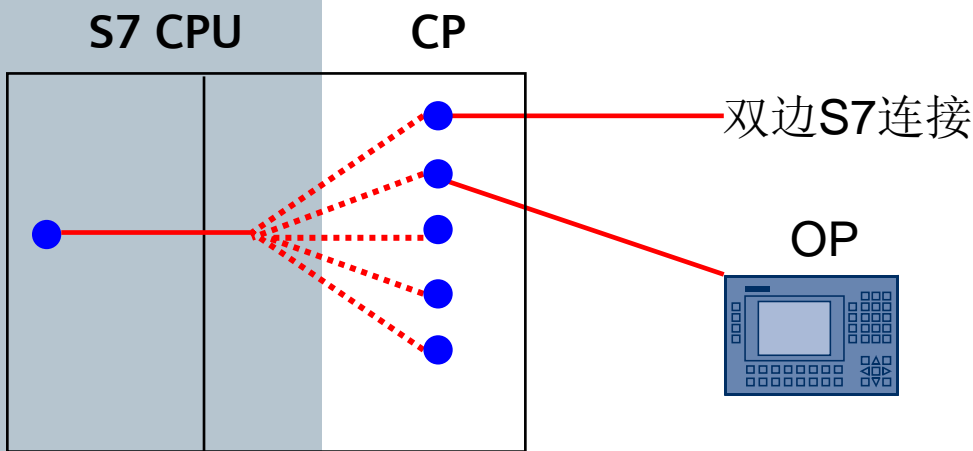
S7-300CP多路复用

- 由于S7-300CPU中S7连接资源数的限制，当通过CP板进行S7相关的通讯服务时可以激活多路复用功能。
- 集成PN接口的CP支持连接资源多路复用，也就是所有组态的双边的S7连接只占用CPU中的一个连接资源，组态后会自动激活多路复用功能。
- 只要激活连接复用，就会预留且仅占用一个CPU连接资源，即使还没有组态该连接。



S7-300CP多路复用

- 连接多路复用只为完全定义的双边的S7连接和 workstation OP。
- 当组态OP进行多路复用时，需要指定CP板所在的槽号。



● S7连接资源

Module Information - CPU 319-3 PN/DP

Path: NetProE_CP\SIMATIC 300(1)\CPU 319-3 P Operating mode of the CPU: RUN
Status: OK Not a force job

General	Diagnostic Buffer	Memory	Scan Cycle Time	Time System
Performance Data	Communication	Stacks	Identification	
Connection Resources				
Maximum number:	32	Not used:	30	
	Reserved	Occupied		
PG communication:	1	1		
OP communication:	1	0		
S7 basic communication:	0	0		
S7 communication:	0	0		
Other communication:	--	1		
Open communication via Industrial Ethernet				
Connection resources in use:		0		

在Other Communication中显示多路复用,仅占用一个S7连接

S7连接资源-S7-400CP

- S7-400CP卡同样无法按照通讯服务来分配相应的S7连接资源。相应的S7服务共同占用CP所提供的S7连接资源。只能通过CP在线的方式查看CP的S7连接资源的占用状态。S7-400CP不支持多路复用。下图为CP443-1GX20的在线。

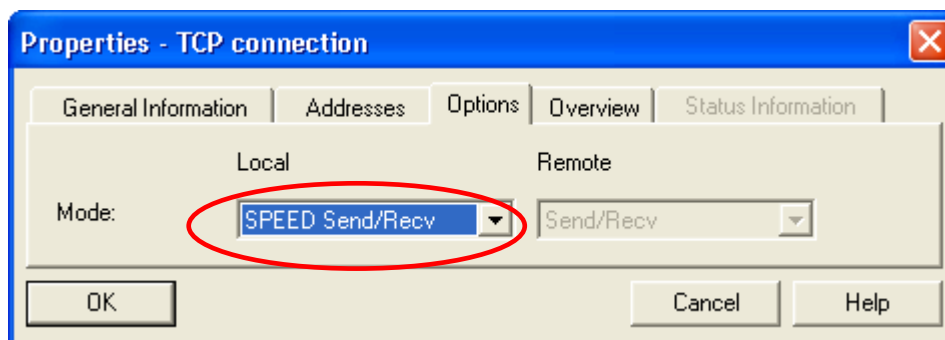
The screenshot shows the 'NCM S7 Diagnostics - CP 443-1 Advanced 0/4 192.168.0.3 ONLINE' window. The left sidebar contains a tree view with 'Statistics of S7 Connections' selected. The main area displays a table titled 'Statistics of the S7 Connections' with the following data:

	Counter	Difference
Maximum connections used:	2	0
Connections currently in use:	2	0
Denied connection establishment attempts:	0	0
Error due to lack of resources:	0	0

A callout box points to the table with the text: 'CP443-1会显示所有的相关于S7通讯的服务'.

S7连接资源-S7-400CP

- S7-400CP443-1GX20支持S5兼容的通讯，可以通过NetPro组态TCP/UDP/ISO on TCP的通讯服务。当使用SPEED SEND/RECV接口模式时，通讯使用FC53AG_SSEND/FC63AG_SRECV功能块。
- 当400CPU启动运行时，会根据每一个SPEED SEND/RECV连接中的通讯任务FC53/FC63初始化连接资源，也就是单纯的组态连接不会占用S7连接资源。
- 每一个SPEED SEND/RECV占用CP443-1的一个S7连接资源，从而占用400CPU的Open IE的一个连接资源。最终占用的还是CPU的一个S7连接资源。



S7连接资源-S7-400CP

Connection status	Local ID	Partner ID	Partner	Type	Active connection partner	Subnet
closed	0001 A050	0001 A050	SIMATIC 300(1) / CPU 319-3 PN/DP	TCP connection	Yes	Ethernet(1) [IE]
Passive connection establishment in progress	0002 A050	0002 A050	SIMATIC 300(1) / CPU 319-3 PN/DP	TCP connection	No	Ethernet(1) [IE]
closed	0003 A050	0003 A050	SIMATIC 300(1) / CPU 319-3 PN/DP	TCP connection	Yes	Ethernet(1) [IE]
Passive connection establishment in progress	0004 A050	0004 A050	SIMATIC 300(1) / CPU 319-3 PN/DP	TCP connection	No	Ethernet(1) [IE]

组态的连接状态与占用S7连接并无直接联系

第一个连接使用SEND/RCV接口
后面3个连接使用SPEED SEND/RCV接口

3个SPEED SEND/RCV连接占用3个S7连接，1个是PG服务占用1个S7连接

3个SPEED SEND/RCV连接占用3个OPEN IE连接，从而占用3个S7连接

NCM S7 Diagnostics - CP 443-1 Advanced 0/4 192.168.0.44 ONLINE

Statistics of the S7 Connections

	Counter	Difference
Maximum connections used:	4	0
Connections currently in use:	4	0
Denied connection establishment attempts:	0	0
Error due to lack of resources:	0	0

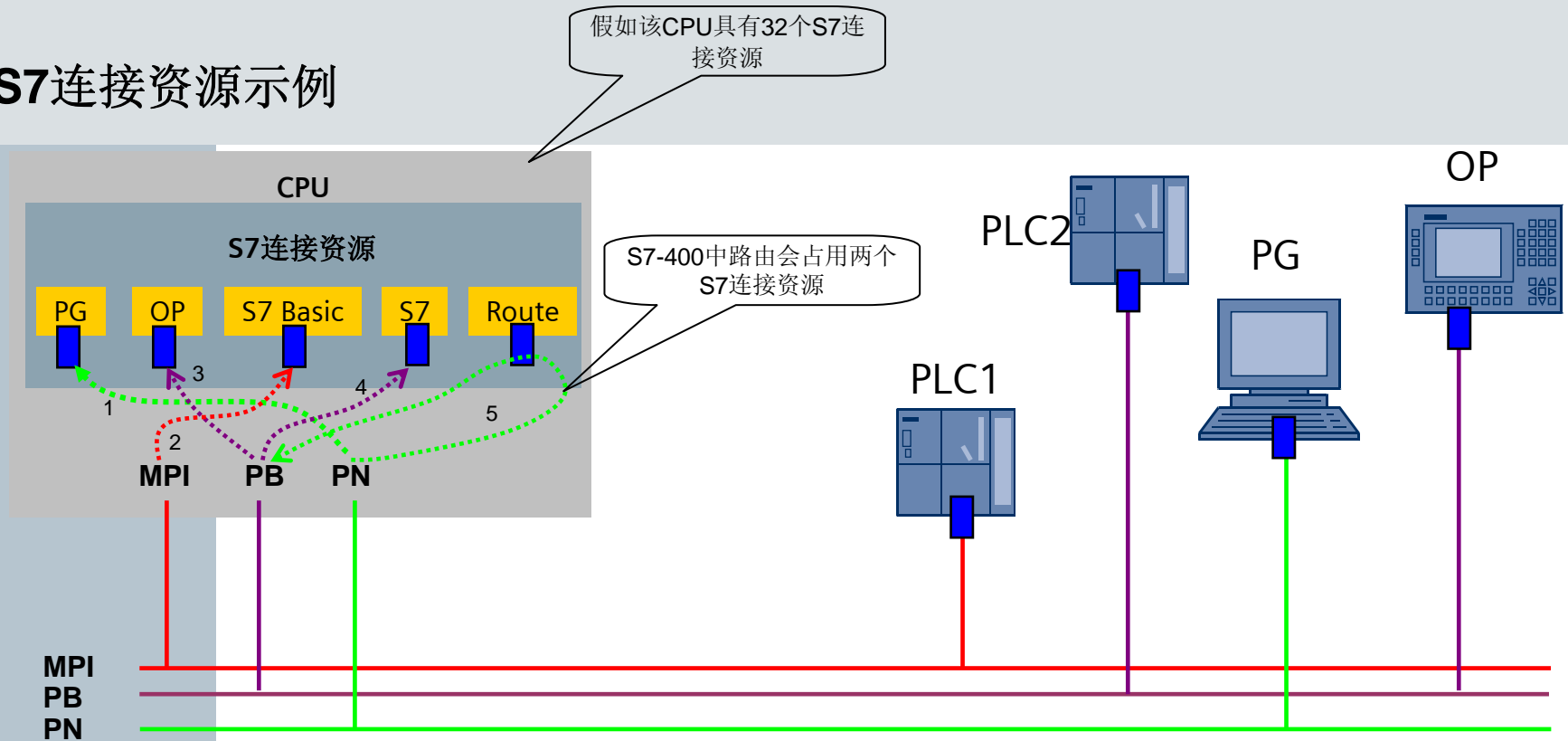
Left sidebar shows: Modules, Industrial Ethernet, Time of day, Operating Mode, C-PLUG, Diagnostic Buffer, Connections, Statistics S/R connections, Statistics of S7 Connections, TCP (TCP connection1, TCP connection5, TCP connection9, TCP connection11), PROFINET CBA.

Module Information - CPU 416F-3 PN/DP

Path: NetProIE_CP\SIMATIC 400(1)\CPU 416F-31 Operating mode of the CPU: RUN
Status: OK Not a force job

General	Diagnostic Buffer	Memory	Scan Cycle Time	Time System
Performance Data	Communication	Stacks	Identification	
Connection Resources				
Maximum number:	64	Not used:	60	
	Reserved	Occupied		
PG communication:	1	1		
OP communication:	1	0		
S7 communication:	0	0		
Other communication:	--	3		
Open communication via Industrial Ethernet				
Connection resources in use:		3		

S7连接资源示例



- 1: PG监控CPU， CPU占用1个PG连接资源；
 - 2: PLC1和CPU通过MPI总线进行S7基本通讯， CPU占用一个S7 Basic连接资源；
 - 3: OP连接CPU进行通讯， CPU占用一个OP的连接资源；
 - 4: PLC2和CPU通过PROFIBUS总线进行S7通讯， CPU占用一个S7的连接资源；
 - 5: PG下载或监控PLC2(从PROFINET总线路由到PROFIBUS总线)， CPU占用一个路由资源。
- 最终对于S7-300CPU剩余27S7连接资源。对于S7-400CPU剩余26个S7连接资源。

S7动态连接和静态连接

S7动态连接:

- 当通讯双方建立通讯关系后，会占用CPU的S7连接资源。当通讯双方断开连接，S7连接资源会被立即释放。
- 动态连接通讯包括PG/OP/S7 Basic/Route/Open IE(S7-400)。
- S7-300CPU中对动态的连接PG/OP/S7 Basic可以预留一定的连接资源，默认的1个PG和1个OP连接资源，这两个连接资源由系统默认，无法被其它的服务所占用。

S7静态连接:

- 当通讯双方建立通讯关系前，通过组态占用CPU的S7连接资源。无论通讯双方通讯与否，当CPU启动后S7连接资源会被永远占用。除非删除该组态的连接。
- 静态连接通讯仅有S7 Connection通讯。

S7连接资源示例

在NetPro中组态S7连接的通讯，组态的S7连接个数占用CPU的S7连接资源数量。

Connection status	Local ID	Partner ID	Partner	Type	Active connection partner	Subnet
Set up	1	1	SIMATIC 300(1) / CPU 319-3 PN/DP	S7 connection	No	Ethernet(1) [IE]
Is being set up	2		Unknown	S7 connection	Yes	Ethernet(1) [IE]

Module Information - CPU 416F-3 PN/DP

Path: NetProE_CP\SIMATIC 400(1)\CPU 416F-3 | Operating mode of the CPU: RUN

Status: OK | Not a force job

Connection Resources	Reserved	Occupied
Maximum number:	64	Not used: 62
PG-communication:	1	1
OP communication:	1	0
S7 communication:	2	1
Other communication:	--	0

Open communication via Industrial Ethernet

Connection resources in use: 0

Buttons: Close, Update, Print..., Help

根据组态预留了2个S7连接资源

成功建立连接表示正在使用其中所预留的S7连接资源

S7通讯任务（Communication Jobs）

- **S7通讯前提需要建立一个S7连接；用户编写S7通讯程序进行一个单方向的通讯即是一个通讯任务。**
- **根据CPU319-3PN/DP的技术数据，一个CPU做多可以组态16个S7连接资源，最多使用32个映像DB或通讯任务。**
- **16个S7连接资源仅仅表示CPU319-3PN/DP可以与对方通讯设备连接的最大数量。而S7通讯任务数量则体现在映像DB的数量上。例如一个通讯任务通过一个PUT功能块建立一个映像DB。映像DB或通讯任务如果超过32，在S7的程序中有错误显示16#14。**
- **如果在一个S7连接中，存在多个S7通讯任务（例如：连接ID=1中存在10个PUT通讯任务），那么其它S7连接的通讯任务会相应的减少（例如：使用剩余的22个PUT或GET通讯任务）。若是一个连接中的通讯任务占满，那么其它的连接的通讯无法建立。**
- **S7-CPU在启动过程中会根据通讯任务进行顺序的初始化，进行连接资源的分配和占用。**

• S7 communication	Yes
– Max. configurable interconnections	16
– Maximum number of instances	32

S7连接的建立和通讯

通过集成PN接口的PLC，例如CPU319-3PN/DP，CPU416-3PN/DP，两者之间通过以太网连接，通过NetPro方式只能建立S7连接。

- 可以使用PUT/GET，USEND/URECV，BSEND/BRECV等FB/SFB(在Communication Blocks和System function blocks库中)来进行编程。
- 通过PUT/GET方式编写程序，不必是单边方式，即S7-300可以不是服务器。

通过集成PN接口的CP，例如CP343-1GX30，CP443-1GX20，两者之间通过以太网连接，建立S7连接需要NetPro方式。

- 需要使用PUT/GET，USEND/URECV，BSEND/BRECV等FB(在SIMATIC_NET_CP库中)来进行编程。

S7-TSAP

一个通讯连接（**S7**或者其它类型的连接）的地址由两个参数定义：

- 第一个参数是本地和远程设备的网络地址，例如**IP**地址。
- 第二个参数是在相应站内的详细地址，例如**Port**号。

对于**TCP**，这个详细的地址通过端口号**Port**来实现，对于**ISO**或者**Profibus**连接，通过**TSAP**来实现。

TSAP (Transport Service Access Point)代表通讯处理器内的源地址。

TSAP也可以用作**S7**连接，但有着一个不同的功能；就是它描述通讯连接的终点。

S7协议的**TSAP**包括2部分：

- 机架和槽号的地址
- 连接资源号

TSAP

连接资源	对象	类型	用于S7连接	意义
0x01	PG	自由连接	No	在每一个CPU预留PG功能
0x02	OP	自由连接	No	在每一个CPU预留OP功能
0x03	其它	自由连接	Yes	主要用于单边连接
0x10~0xDF	动态或静态连接	组态连接	Yes	用于双边的连接

PUT/GET和USEND/URECV的通讯字节数

Own CPU	Remote CPU	Data block size in bytes			
S7-300	Any	240 (S7-300)			
S7-400	S7-300 / C7-300	240 (S7-400)			
S7-400	S7-400 or CPU 318	480			
		<u>Number of used parameters SD I, RD i, ADDR i</u>			
Data block size	SFB/FB	1	2	3	4
240 (S7-300)	PUT/GET/USEND	160	-	-	-
240	PUT	212	-	-	-
S7-300 via integrated interface	GET	222	-	-	-
	USEND	212	-	-	-
240 (S7-400)	PUT	212	196	180	164
	GET	222	218	214	210
	USEND	212	-	-	-
480	PUT	452	436	420	404
	GET	462	458	454	450
	USEND	452	448	444	440

PUT/GET和USEND/URECV的通讯字节数

以下描述假定S7-300例如CPU319-3PN/DP作为一方进行S7通讯：

- Data block size就是S7协议的数据单元，简称PDU。
- PDU表示S7通讯的Data数据块的最大尺寸，对于S7-300PLC来说在以太网上传输的最大数据块PDU的尺寸为240Bytes。
- PDU的前28个字节用于数据传输的起始信息，剩余的字节例如212bytes是用户数据。
- 对于PUT/GET， USEND/URECV。SD_1或RD_1的最大传输数据为212Bytes。也就是在编程时最多可以编写212bytes用于传输。
- 当使用SFB编写S7程序时，注意不要编写RD_2和ADDR_2或其它，否则RD_1的最大的数据长度则为160。只有重新生成SFB15”PUT”的背景数据块才能传输最大212Bytes。
- 上述原因建议用户在编写S7-300的S7程序时，使用Communication Blocks库中的FB功能块。

BSEND/BRECV和USEND/URECV的区别

- 除了传输字节数量上的不同，主要是**USEND/URECV**在应用层上没有应答。而**BSEND/BRECV**则在应用层具有应答。
- 从侧面上反映了两者在**S7**协议层上的应用协议不同。
- 理论上，**USEND**比**BSEND**的传输速度快，但是由于**USEND**在通讯字节上的限制，所以两者应用对比没有太大的意义。
- 在同一连接资源下，**BSEND/BRECV**通过**R_ID**对应进行通讯，如果使用**USEND/URECV**也同样是用在同一连接资源下时，对应的**R_ID**一定要与上述不同。