#### 1.1 测试环境简介



图3-5工业控制系统信息安全实验平台的拓扑结构

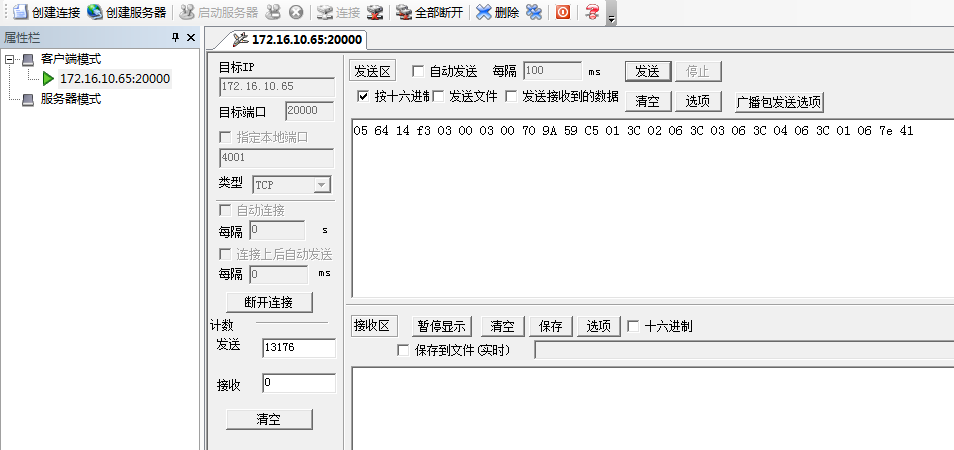
如图3-5工业控制系统信息安全实验平台的拓扑结构，测试环境，包括防护模块规则配置端，模拟攻击端，PLC监控端，防护模块，以及模拟控制端。防护模块规则配置端可以实现对防护模块的访问控制规则以及深度包检测规则的配置。根据不同的工业控制协议，我们分别在模拟供给端和模拟控制端，安装基于不同工业控制协议的客户端与服务器端软件。模拟进行基于工业控制协议的通信过程。通过发送不同的数据包来观察防护模块对于不同数据包检测与防护能力。

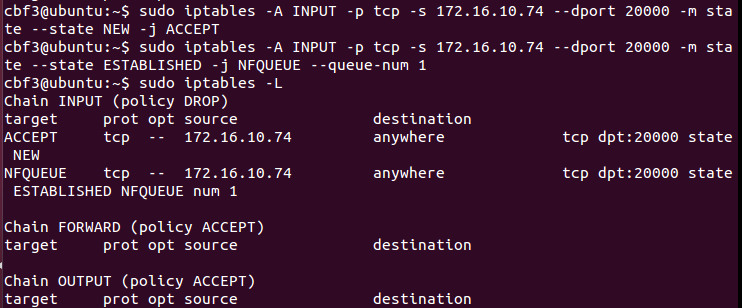
#### 1.2基于DNP3.0协议的测试

试验测试通过分别在模拟攻击端和模拟控制端分别安装DNP3.0客户端软件与服务器软件建立通信过程，客户端发送数据包通过工业控制防护系统到服务器端来进行验证。

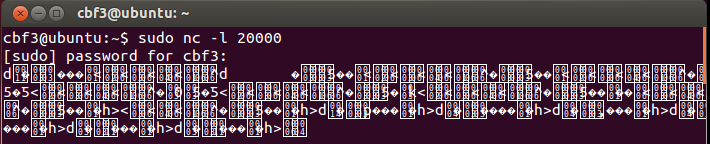
#### 1.3测试步骤

（1）建立连接

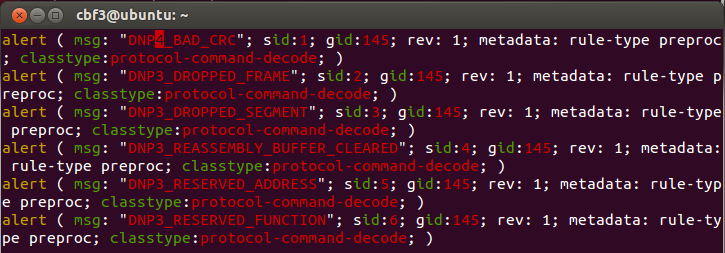




1. 数据监听



1. DNP预处理规则



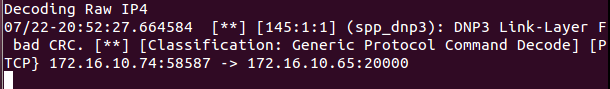
对应描述：

SID Description-------------------------------------------------------------------- 1 A Link-Layer Frame contained an invalid CRC. (Enable "check\_crc" in the preprocessor config to get this alert.) 2 A DNP3 Link-Layer Frame was dropped, due to an invalid length. 3 A Transport-Layer Segment was dropped during reassembly. This happens when segments have invalid sequence numbers. 4 The DNP3 Reassembly buffer was cleared before a complete fragment could be reassembled. This happens when a segment carrying the "FIR" flag appears after some other segments have been queued. 5 A DNP3 Link-Layer Frame uses an address that is reserved.

6 A DNP3 request or response uses a reserved function code.

#### 1.4测试方法

（1）针对SID1:检验码



针对SID3:序列号

正确数据：

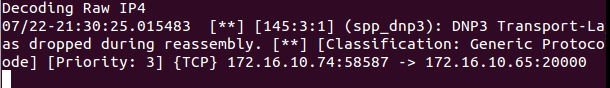
05 64 14 f3 03 00 03 00 70 9A **D9** C5 01 3C 02 06 3C 03 06 3C 04 06 3C 01 06 06 5E

主要改动：

05 64 14 f3 03 00 03 00 70 9A **19** F5 01 3C 02 06 3C 03 06 3C 04 06 3C 01 06 5F 07

05 64 14 f3 03 00 03 00 70 9A D9 C5 01 3C 02 06 3C 03 06 3C 04 06 3C 01 06 06 5E

05 64 14 f3 03 00 03 00 70 9A 19 F5 01 3C 02 06 3C 03 06 3C 04 06 3C 01 06 5F 07



针对SID4：缓冲区

05 64 FF 44 03 00 03 00 29 E7 99 A5 81 00 00 01 02 01 00 00 EC 00 01 01 01 01 6D DB 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 BB C3 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 BB C3 01 01 01 01 01 01 01 01 01 01 81 81 81 81 81 01 18 F1 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 BB C3 01 01 01 01 01 01 01 01 01 01 01 01 81 01 81 81 F4 72 81 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 B7 F4 81 01 01 01 81 01 01 01 01 01 01 01 01 01 01 01 F0 FF 01 01 01 01 81 01 81 81 01 01 01 01 01 01 81 01 06 11 01 01 81 01 01 01 01 01 01 01 01 01 01 01 01 01 9A 4A 01 01 81 01 01 01 81 01 01 01 01 01 01 01 01 01 46 83 01 01 01 01 01 01 01 81 81 81 01 81 01 01 01 81 84 DC 81 01 01 01 81 81 01 01 01 81 81 01 01 01 81 81 1E CE 01 01 01 81 81 01 01 01 81 81 01 01 01 81 81 01 45 85 01 01 81 01 01 01 01 01 81 01 01 01 81 81 01 01 50 3C 01 81 81 01 01 01 81 81 01 01 4E 06 59 ``````````

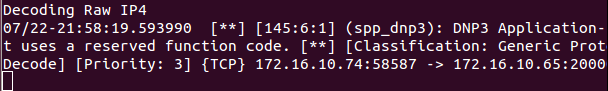
针对SID6：保留功能代码

正确数据：

05 64 14 f3 03 00 03 00 70 9A D9 C5 01 3C 02 06 3C 03 06 3C 04 06 3C 01 06 06 5E

主要改动：

05 64 14 f3 03 00 03 00 70 9A D9 C5 EE 3C 02 06 3C 03 06 3C 04 06 3C 01 06 31 32

****

05 64 14 f3 03 00 03 00 70 9A D9 C5 17 3C 02 06 3C 03 06 3C 04 06 3C 01 06 B1 17(用保留的也是会报错的）

#### 1.5总结

通过实验测试可知，该防护模块基于DNP3.0协议，对于协议内容中检验码、长度、序列号、缓冲区等做全面的深度包解析，实现访问控制和通信管理,从而有效的实现防护功能。