ntop

Relazione del Progetto di Gestione di Reti
Estensione di nDPI con Modbus
Anno 2017/2018

Francesco Sciulli Matricola 516740

21/11/2018

Indice

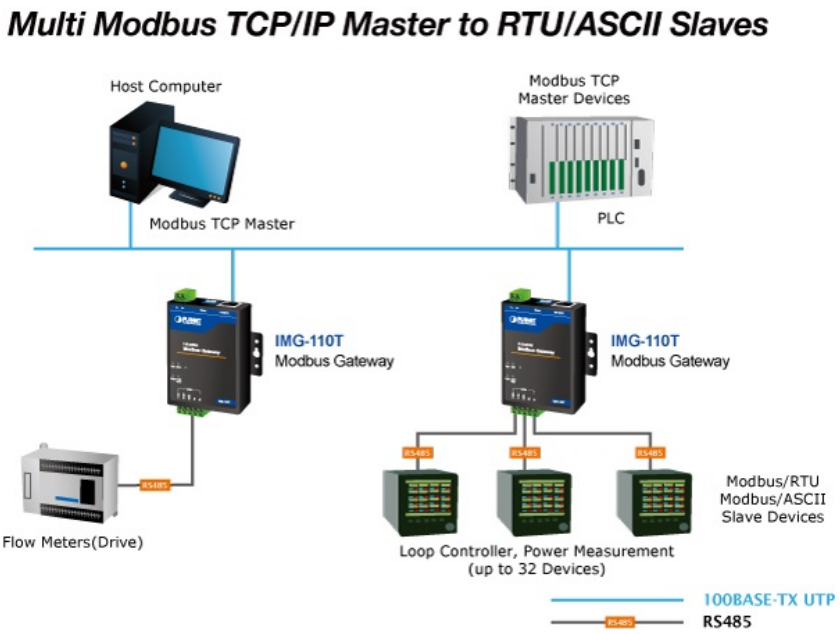
1 Introduzione

1.1 nDPI

nDPi è una libreria scritta in C utilizzata per effettuare Deep Packet Inspection.

1.2 Che cosa è Modbus?

Modbus è un protocollo di comunicazione seriale creato nel 1979 da Modicon per mettere in comunicazione i propri controllori logici programmabili (PLC). È diventato uno standard di fatto nella comunicazione di tipo industriale, ed attualmente è uno dei protocolli di connessione più diffusi al mondo fra i dispositivi elettronici industriali.



Le ragioni che lo hanno portato ad un elevato utilizzo da un'alta quantità di utenti sono le seguenti:

- Progettato pensando a utilizzi industriali
- È un protocollo pubblicato apertamente e royalty-free
- Semplicità di installazione e mantenimento
- Muove raw bits e words senza porre molte restrizioni ai produttori

Modbus consente la comunicazione fra diversi dispositivi connessi alla stessa rete. E' spesso usato per connettere un computer supervisore con un'unità terminale remota (RTU) nel controllo di supervisione e sistemi di acquisizione dati (SCADA).

Esistono due versioni del protocollo: su porta seriale e su Ethernet.

1.3 Comunicazione tra Master e Slave

II protocollo MODBUS definisce il formato e la modalità di comunicazione tra un "master" che gestisce il sistema e uno o più "slave" che rispondono alle interrogazioni del master.
Si possono connettere un master e fino a 247 slave (limite teorico).
Solo il master può iniziare una transazione.
Una transazione può avere il formato domanda/risposta diretta ad un singolo slave o broadcast in cui il messaggio viene inviato a tutti i dispositivi sulla linea che non danno risposta.

1.4 Modbus su linea seriale

Ci sono due differenti protocolli su linea seriale e sono Modbus ASCII e Modbus RTU.

- Il formato ASCII è facilmente leggibile e ridondante e usa un checksum di tipo LRC (Longitudinal redundancy check)
- Il formato RTU fa seguire ai comandi/dati un campo checksum di tipo CRC (Cyclic redundancy check).

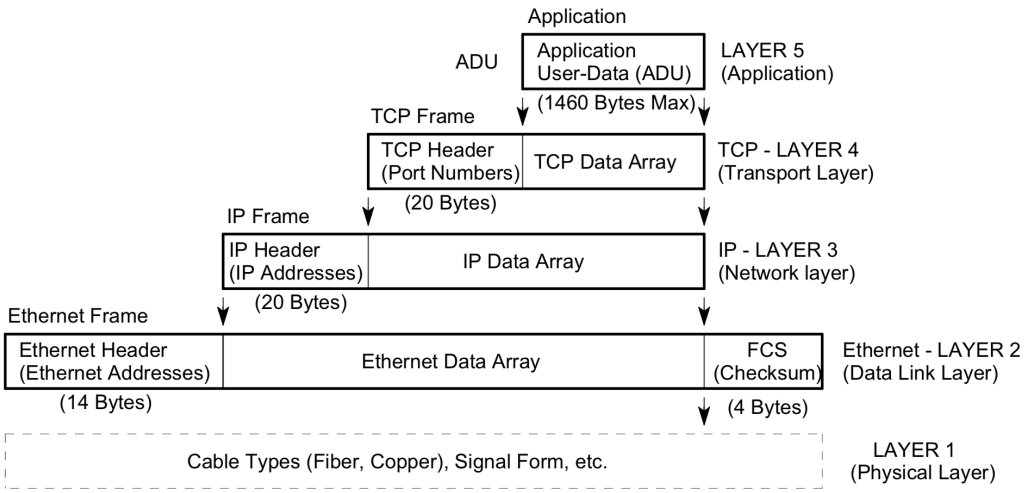
I nodi configurati per la variante RTU non possono comunicare con nodi configurati per l'ASCII e viceversa.

2 Modbus TCP/IP

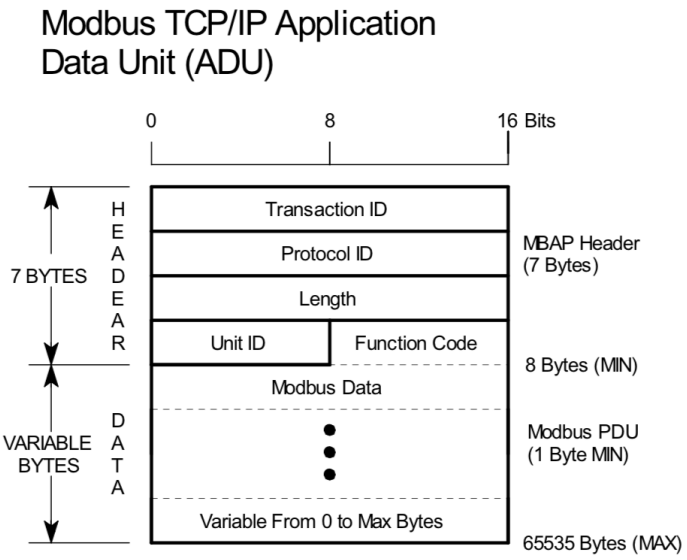
2.1 Protocollo

Modbus/TCP è molto simile al Modbus RTU, ma trasmette i pacchetti del protocollo dentro pacchetti di dati TCP/IP.

Figure 1: CONSTRUCTION OF A TCP/IP-ETHERNET DATA PACKET



Modbus/TCP è caratterizzato dai campi mostrati in figura.



Come tutti i protocolli standard di livello applicativo anche Modbus utilizza una porta prefissata (502) che appartiene al range delle porte riservate [da 0 a 1023].

2.2 Campi dell'Header

- Transaction/invocation Identifier (2 Byte): Questo campo è usato per transazioni appaiate quando messaggi multipli sono inviati lungo la stessa connessione TCP da un client senza attendere la risposta dal server.
- Protocol Identifier (2 byte): Questo campo è sempre 0 per Modbus e altri valori sono riservati per future estensioni.
- Length (2 byte): Questo campo è un counter dei byte dei campi rimanenti includendo unit identifier byte, function code byte, e i campi dati.
- Unit Identifier (1 byte): Questo campo è usato per identificare un server remoto collocato non in una rete TCP/IP (su comunicazione seriale).

3 Implementazione

3.1 Caratteristiche di un pacchetto Modbus

Affinché il dissector riconoscesse il pcap di Modbus come tale ho analizzato il pacchetto e ho controllato alcune caratteristiche tipiche del Pacchetto Modbus.

I controlli che ho fatto sono i seguenti :

- il pacchetto doveva stare in un segmento TCP
- la lunghezza del payload del segmento TCP deve essere almeno 8 byte
- il segmento deve essere inviato o deve essere ricevuto sulla porta 502
- il campo lenght deve contenere la lunghezza del payload del segmento meno la dimensione dell'header del pacchetto di livello applicativo

4 Istruzioni per la compilazione e l'utilizzo

4.1 Operazione preliminare

La cartella contenente il codice è compressa in un file zip e prima di poter essere utilizzata deve essere estratta mediante il comando

- unzip nDPI-dev.zip

4.2 Compilazione ed Esecuzione

Essendo un estensione di nDPI il programma adotta le medesime istruzioni fornite dal sito: `https://github.com/ntop/nDPI`

Le operazioni da eseguire sono le seguenti

1) ./autogen.sh
2) ./configure
3) make
4) cd tests
5) ./do.sh

4.3 Risultati di Modbus

E' possibile controllare che Modbus sia rilevato correttamente tramite le operazioni seguenti

1) cat tests/result/Modbus.pcap.out
2) cd ..
3) cd example
4) ./ndpiReader -i ../tests/pcap/Modbus.pcap -v 1

4.4 Alternative

E' possibile eseguire le operazioni di 4.2 e di 4.3 tramite i due script scritti da me direttamente nella directory principale

- ./run.sh (analogo a 4.2)
- ./Modbuscheck.sh (analogo a 4.3)