

Industrijska komunikacija

**Simon Vrbnjak
Lapp Slovenija,
Industrijska komunikacija, Profinet topologija,
Industrijska mrežna infrastruktura za varno in zanesljivo avtomatizacijo
simon.vrbnjak@lappslovenia.com**

Industrial communication

What is Centralized and decentralized network. Definition of PROFINET topology and glance of other protocols. Difference between PROFINET and Profibus. How does PROFINET and NAT switch work. OSI model and communication channels. Why do we need conformance classes.

Kratek pregled prispevka

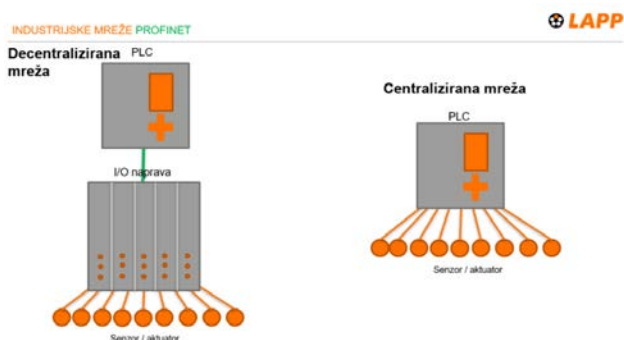
Kaj so centralizirane in decentralizirane mreže. Definicija PROFINET protokola in pregled ostalih protokolov. Razlike med PROFINET in Profibus protokolom. Kako delujejo PROFINET in NAT stikala. OSI model in komunikacijski kanali. Zakaj potrebujemo razrede skladnosti.

1 Industrijska komunikacija

Podjetje LAPP, strokovnjak na področju kablov in kablskih sistemov, si utira pot tudi v industrijski komunikaciji. Smo eden vodilnih ponudnikov rešitev na področjih avtomatizacije, robotike, prehrabene in pakirne industrije, e-mobilnosti, itd. Tokrat bomo predstavili segment komunikacije v avtomatiziranem procesu.

Pri vsaki avtomatizirani aplikaciji morajo vsi udeleženci komunicirati med seboj, torej potrebujemo industrijsko mrežo.

Industrijske mreže delimo na centralizirane in decentralizirane (slika 1).



Slika 1: Decentralizirana in centralizirana industrijska mreža.

Decentralizirana rešitev je trenutno najbolj razširjena v industriji. Malokdo se še odloči za centralizirano rešitev, saj ta predstavlja ogromno naporov in stroškov pri polaganju kilometrov kablov. Prav tako otežuje reševanje okvar, saj smo v primeru le-teh primorani menjati celotno linijo.

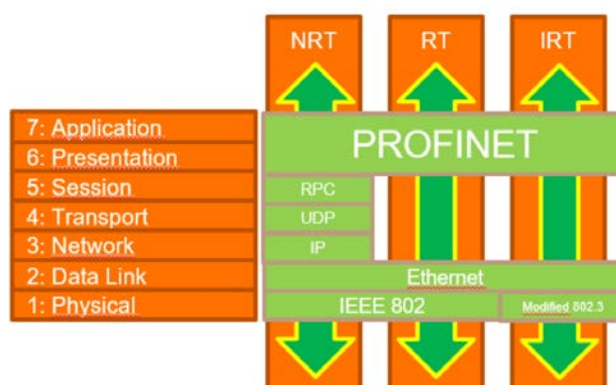
Pri centralizirani rešitvi so PLC (PLC – Programabilni Logični Računalnik) inženirji primorani vse senzor/aktuator povezave peljati iz proizvodnje naravnost do PLC-jev. Danes lahko vgradimo vhodne in izhodne module v neposredno bližino senzorjev in aktuatorjev v proizvodni hali in jih povežemo s primernimi senzor/aktuator kabli krajših dolžin. Drugi konec pa povežemo s kontrolno sobo s samo enim kablom. To lahko dosežemo tako, da med kontrolno sobo, kjer se sedaj nahaja naš PLC in

proizvodnjo vgradimo še I/O oz. vhodno/izhodno napravo.

V proizvodnji vsako senzor/aktuator napravo, (servo-pogoni, pozicionerji, itd.) povežemo s svojo I/O kartico na I/O napravi (najbolj razširjena je ET200SP Siemens), nato to I/O napravo povežemo z oddaljeno I/O napravo v kontrolni omarici. Slednjo povežemo s PLC-jem. Senzor/aktuator povezave potrebujejo vsaka svoj senzor/aktuator kabel, medtem ko I/O naprave in PLC-je med seboj povezujemo le z enim kablom. Odvisno od projekta lahko uporabimo različne industrijske topologije. V Evropi sta najbolj razširjeni PROFINET in PROFIBUS.

1.1 PROFINET topologija

PROFINET topologija uporablja veliko protokolov, da zapolni model OSI (slika 2). Vsak od teh protokolov ima nekaj podatkov, ki jih je treba poslati med komunikacijske partnerje.



Slika 2: OSI model (OSI – Open Systems Interconnection).

OSI model sestavlja 7 plasti. Najbolj temeljna plast je fizična plast. Komunikacija na tej plasti poteka v različnih oblikah. Lahko gre za elektrone, ki se pretakajo po žici, radijske valove, ki se premikajo po zraku, ali fotone, ki potujejo skozi optična vlakna.

Obstaja več načinov kako izvesti fizično plast. Protokol PROFINET uporablja plasti OSI

modela že desetletja. Programski paket IEEE 802 zajema to, kar za nas predstavlja žični Ethernet (802.3) in brezžični Ethernet (802.11).

PROFINET je določil že znan standard 802.3 Ethernet za plast podatkovne povezave. To pomeni, da ima vsaka naprava PROFINET svoj MAC (Media Access Control) naslov.

Na plasti mrež lahko PROFINET uporablja za nekatere komunikacije protokole IP (Internet Protocol), UDP (User Datagram Protocol) in RPC (Remote Procedure Call). Ti protokoli imajo dodatne zahteve (več bajtov na žici, več časa obdelave pri viru in cilju), zato jih PROFINET v uporabo pokliče le, kadar je to nujno potrebno.

Imajo pa nekaj relevantnih prednosti, kot so vse informacije o naslovih, ki so zapakirane v paket UDP / IP.

MAC, IP naslove in vrata UDP lahko uporabimo za preklon, usmerjanje in obdelavo podatkov PROFINET.

PROFINET mrežo sestavljajo:

Krmilnik (v PROFIBUS terminologiji to predstavlja class-1 master)

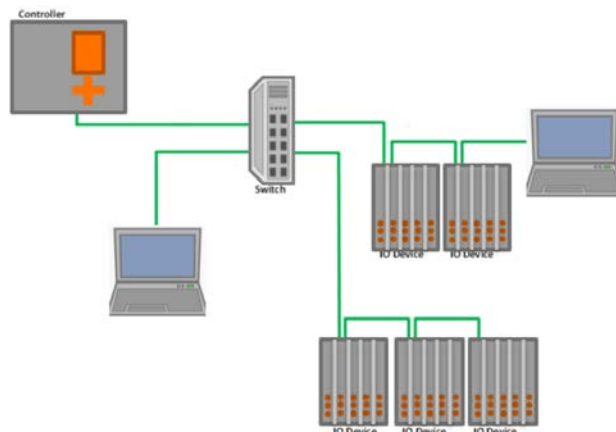
- PLC = Programabilni Logični Računalnik,
- DCS = Distribucijski Kontrolni Sistem,
- PAC = Programabilni Krmilnik za Avtomatizacijo;

Naprave/Stikala (v PROFIBUS terminologiji to predstavlja slave)

- I/O bloki, sistemi nadzora, RFID čitalci, pogoni, procesni instrumenti, proksiji ali celo drugi krmilniki, ki so povezani v mrežo PROFINET;

Nadzorniki (opsijsko)

- to so programabilne naprave, PC-ji ali vmesniki človek – stroj (HMI – Human Machine Interface), ki se uporabljajo za diagnostiko;



Slika 3: PROFINET topologija.

Osnovna naloga topologije PROFINET je hitra in deterministična izmenjava podatkov. Se pravi podatki pridejo na cilj takrat, ko se jih potrebuje. Hitrosti določajo aplikacije, procesni instrumenti se posodobijo v stotinah milisekunde (tovarne dosegajo <10 milisekund). Še bolj zahtevna pa je sinhronizacija nadzora gibanja.

Ostale topologije in protokoli niso tako hitri in deterministični ali pa spadajo v zaprte mreže:

- **Modbus TCP:** uporablja TCP (Transmission Control Protocol), ki zahteva, da je virtualna povezava vzpostavljena med dvema napravama, tako morajo sporočila – podatki skozi TCP/IP (Transmission Control Protocol / Internet Protocol) sklad,
- **Ethernet/IP:** uporablja UDP (User Datagram Protocol), taka sporočila – podatki potekajo skozi UDP/IP sklad. Čas skozi sklad je variabilen, s tem se zmanjša hitrost in posledično determinističnost.
- **EtherCAT:** je deterministična, vendar zaprta mreža.

1.2 PROFINET promet

Poleg sporočil – podatkov se izmenjujejo tudi kvaliteta in opravljanje informacij. Torej ne dobimo samo prenosa podatkov temveč tudi informacijo ali je podatek prispel nepoškodovan. S tem dosežemo proaktivno vzdrževanje, podatke pa lahko prenašamo z vnaprej definiranim režimom.

1.2.1 Kako PROFINET prenaša informacije

Najprej si odgovorimo na naslednja vprašanja:

- kakšne informacije želimo prenašati,
- ali jih potrebujemo takoj,
- so varnostno kritične,
- ali gre za velike pakete, ki jih moramo poslati v enem kosu.

Za različne scenarije imamo različne rešitve, imenovane komunikacijski kanali:

- realni čas (RT – Real-Time),
- nerealni čas (NRT – Non-Real-Time),
- izohroni realni čas (IRT – Isochronous Real-Time).

RT

Kadar govorimo o industrijskih protokolih za avtomatizacijo, mora prenos podatkov potekati v realnem času. Okvirji (frames) se izmenjujejo v RT kanalu z majhno zakasnitvijo in nizkimi variancami (jitter). Slaba stran tega je, da nimamo IP naslova, zato se RT okvirji ne morejo prenašati med lokalno mrežo (LAN – Local Area Network).

NRT

Se uporablja za diagnostična orodja potrebna za dostop do PROFINET naprav, da

lahko te vodijo zapise o stanju mreže PROFINET. Uporablja se v vseh plasteh OSI modela (slika 2) in ima IP naslov. Tako lahko PROFINET nadzorniki dostopajo do naprav navzkrižno ali celo preko interneta. Slaba stran NRT je, da prihaja do večjih zakasnitev in varianc (jitter).

IRT

Znano je, da lahko stikala delujejo kot prometna križišča, ki usmerjajo več tokov podatkov do ene same povezave. Tako kot gneča v križiščih, lahko tudi stikala povzročijo nepričakovane zamude v prometu podatkov.

PROFINET ima veliko razredov:

- razredi skladnosti (conformance classes),
- razredi redundance medijev (media redundancy classes),
- itd.

Pozornost bomo namenili razredom realnih časov in njihovem delovanju v PROFINET-u.

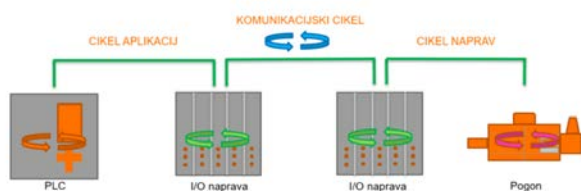
Razredi RT določajo:

- katere storitve bodo uporabljene in kako bo deloval protokol v realnem času, če bo komunikacija (časovno) sinhronizirana ali nesinhronizirana med napravami,
- Katera pot bo izbrana v napravi ali mreži in ali bo morda potrebna strojna podpora, kot recimo PROFINET ASIC (Application Specific Integrated Circuit – integrirano vezje specificirano za aplikacijo) ali FPGA (Field Programmable Gate Arrays – programabilni nizi vrat).

Vse PROFINET naprave morajo podpirati RT, kar običajno pomeni okoli 250 mikrosekund do 10 milisekund časa posodobitve z <100 mikrosekund varianc (jitter), podatki pa so poslani nesinhrono.

RT aplikacije običajno niso sinhrono:

- Različni, ne-sinhroni cikli
- Aplikacije, podatkovni promet in naprave imajo svoje cikle

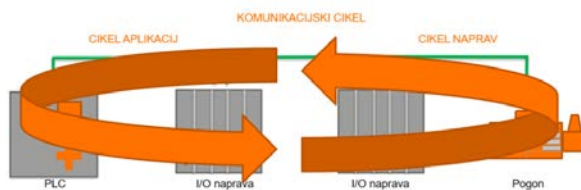


Slika 4: RT cikli.

1.2.1.1 Časovno sinhroniziran prenos podatkov

Časovno sinhroniziran prenos podatkov:

- Različni, ne-sinhroni cikli
- Aplikacije, podatkovni promet in naprave so sinhronizirane
- Cikli časov so zmanjšani na 250 µs z optimalnimi variancami (jitter) < 1µs
- Za večje hitrosti I/O in nadzore gibanj aplikacij



Slika 5: Časovno sinhronizirani cikli.

Kadar govorimo o RT, moramo razumeti, da se uporablja poseben EtherType (0x8892) za PROFINET, ki predstavlja RT sporočilo z uporabo standardnih Ethernet komponent in omogoča preskakovanje TCP/IP plasti za podatkovni proces aplikacij RT.

Pri večini aplikacij bo to delovalo brez težav. To velja tudi za razrede skladnosti CC-A in CC-B.

V IRT so časi ciklov običajno <1 milisekunda z 1 mikrosekundo varianc (jitter). Uporabljajo se v aplikacijah za nadzor gibanja, kjer več naprav potrebuje časovno sinhronizacijo in višjo stopnjo zanesljivosti z uporabo rezervacije pasovne širine in urnika.

V razredu skladnosti C (CC-C) naprave podpirajo IRT in RT. Ta razred omogoča tudi storitev RT z uporabo UDP/IP (User Datagram Protocol/Internet Protocol). Ne poznamo veliko proizvajalcev, ki bi to uporabljali, predvsem

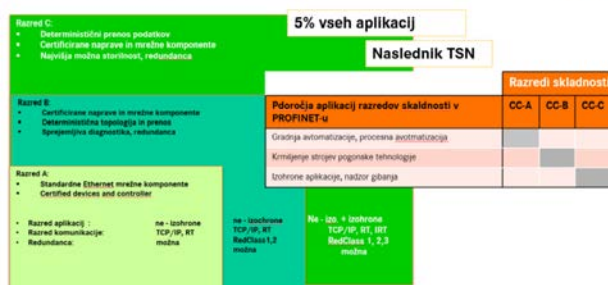
zaradi tega ker je RT/IRT veliko bolj robusten, zanesljiv in enostavnejši za uporabo.

Pri uporabi UDP/IP lahko pričakujemo več zamud in nepotrebnih stroškov. Seveda pa lahko RT okvirje prenašamo tudi z usmerjevalnikom (router).

Večina PROFINET prometa poteka preko stikal samo na delu sistema PROFINET, saj RT/IRT uporabljajo UDP ali TCP, zato se jih lahko uporabi preko usmerjevalnika in stikala (npr. konfiguracija in diagnostika). Za razvijalce so RT razredi določeni v GSD datoteki ali v konfiguracijskem orodju krmilnikov (tag = SupportedRT_Classes).

Na voljo imamo torej:

- RT_CLASS_1 = RT (za razred skladnosti A in B)
- RT_CLASS_2 = IRT (se danes ne uporablja pogosto)
- RT_CLASS_3 = IRT (uporablja se, kadar so potrebne aplikacije za gibanje ali visoke hitrosti, razred skladnosti C).



Slika 6: Razredi skladnosti.

2 Industrijska mrežna infrastruktura za varno in zanesljivo avtomatizacijo

Zaradi potreb po učinkovitosti, količina podatkov vedno bolj narašča, s tem se posledično večja tudi potreba po višjih standardih za kibernetsko varnost. Prav tako

raste potreba po mrežni infrastrukturi, saj so industrijski sistemi vse bolj avtomatizirani.

Rešitev za to predstavljajo Ethernet oz. PROFINET stikala, Fieldbus in NAT prehodi oz. zavarovani spletni dostopi.

Za optimalno delovanje industrijskih mrežnih infrastruktur potrebujemo zanesljive in fleksibilne rešitve, ki bodo enostavne za rokovanje, ne glede na aplikacijo. Ne samo da bodo bolje reševale naloge, temveč bodo tudi bolj kompaktne, torej bolj prijazne za vgradnjo v kontrolne omare. Tako je LAPP v sodelovanju z renomiranim nemškim podjetjem na področju mrežne tehnologije, Helmholz GmbH, razvil stikala in komplementarna programska orodja, ki so se izkazala kot zelo prijazna do naših uporabnikov. [3]

2.1 Ethernet in PPROFINET stikala

Komunikacija med krmilniki, PLC-ji in ostalimi komponentami poteka preko stikal. Slednja spadajo med najpomembnejše mrežne komponente. Še tako majhne spremembe, kot recimo optimizacija, občutno vplivajo na te komponente. To velja tudi za dizajn, saj se neprestano soočamo s prostorsko stisko znotraj kontrolnih omaric.

2.1.1 Neupravljana stikala

Neupravljana Ethernet stikala podjetja LAPP postavljajo nove standarde glede dimenzij. Stikala s štirimi vrati merijo v širino samo 49 mm, z osmimi vrati pa samo 65 mm. Zahvaljujoč obliki, ki je izredno kompaktna, jih lahko uporabimo v različnih industrijskih aplikacijah. Lahek in še vedno robusten dizajn je primeren in enostaven za instalacijo na DIN letev. Ko stikala enkrat fizično povežemo so že pripravljena za operacije. Vse lahko uredimo praktično brez orodij.



Slika 7: Neupravljanost stikala.

2.1.2 PROFINET stikala

Previdni moramo biti pri uporabi konvencionalnih Ethernet stikal v povezavi s PROFINET mrežami, saj-le ta ne nudijo določanja prioritetenj okvirjev ter njihovih podatkovnih velikosti v industrijskih mrežah.

Za takšne potrebe je bolj primerno uporabiti PROFINET stikala. Ena izmed bistvenih funkcij takšnega stikala je ravno določanje prioritetenj okvirjev v omrežju. Upravljanost stikala lahko ugotovi ali gre za spletno poizvedbo, FTP podatkovni prenos, medijski promet ali PROFINET okvir. V primeru prenosa velikih paketov ali prioritetenj okvirjev lahko sedaj določimo njihovo prioriteto in s tem preprečimo izgubo okvirjev. To pomeni, da je potrebna jasna in nedvoumna segmentacija med Ethernetom in PROFINET-om.

Skoraj tako pogosto kot stikala se uporabljajo tudi fieldbus gateway-i, s katerimi povezujemo individualne mreže v avtomatizaciji. Ne glede kje, v kateri bus mreži (PROFINET, CANopen, DP) jih uporabimo, je pomembna velikost. Denimo LAPP PROFINET gateway zavzame le četrtnino prostora v primerjavi s konvencionalnimi rešitvami drugih proizvajalcev. Pri sami instalaciji LAPP

PROFINET stikala pa ne potrebujete dodatnega programskega orodja.



Slika 8: PROFINET stikalo.

2.2 Fieldbus in NAT stikala

Pri prehodu na Ethernet mreže ne smemo zanemariti kibernetike varnosti. Slednja postaja vedno bolj pomembna, saj so vdori vse bolj pogosti in rastejo zaradi naših potreb po vedno večjih količinah prenosov podatkov. Zato priporočamo, da se naše mreže loči na segmente. Pri tem je osrednja naloga varna vključitev strojnih omrežij v proizvodno omrežje višje ravni. LAPP ponuja rešitev z NAT usmerjevalnikom s funkcijo požarnega zidu.

2.2.1 ETHERLINE[®] ACCESS NF04T NAT/Firewall

NAT usmerjevalnik ima 4, 8 ali 16 RJ45 vrat. Prva od teh vrat so WAN vrata za mreže višjega nivoja, sledijo LAN vrata za mreže na nivoju strojev. Naloga NAT stikala je preprečiti neavtoriziran dostop do strojne mreže. Zahvaljujoč individualni konfiguraciji se požarni zid enostavno prilagodi zahtevam strojne mreže. Če želimo realizirati enak IP naslovni razpon, ga lahko uporabimo tudi kot most.



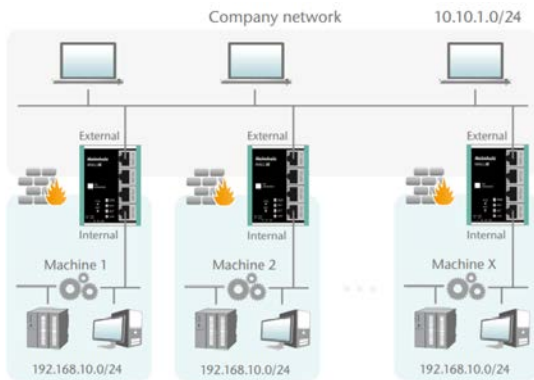
Slika 9: ETHERLINE[®] ACCESS NF04T NAT/Firewall stikalo.

Tudi ta je v izredno majhnem kompaktnem ohišju. Uporabi se ga lahko v treh možnih načinih delovanja:

- **Osnovni NAT:** stikalo uporablja NAT (NAT – Network Address Translation) operacije za podatkovni promet med različnimi IPv4 mrežami (OSI model – plast 3).

Omogoča prevajanje naslova preko NAT in uporablja paketne filtre za omejitev dostopa do avtomatiziranega omrežja, ki se nahaja zadaj. Osnovni NAT, znan tudi kot "1:1 NAT" ali "Static NAT", je prevod posameznih naslovov IP, ali celotnih obsegov naslovov. Prevajanje poteka izključno na ravni IP, kar pomeni, da je vsa vrata mogoče nasloviti brez izrecnega posredovanja.

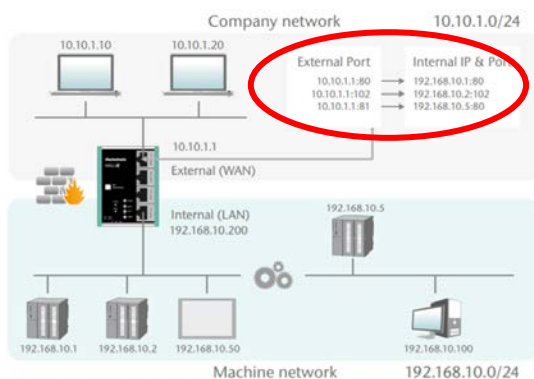
Če posplošimo, stikalo NAT s 4 vrati uporablja NAT za dodeljevanje unikatnega IP naslova in treh naslovnih območij zunanega omrežja WAN za vsak IP naslov v internem omrežju LAN. Tako lahko povežemo veliko strojev in računalnikov s proizvodno mrežo in obdržimo unikatni IP naslov iz zunanega omrežja.



Slika 10: Osnovni NAT [3].

- **NAPT:** Prevajanje mrežnih naslovov in vrat NAPT (Network Address and Port Translation), znanih tudi kot "1:N NAT" ali "Masquerading – maskiranje", se uporablja takrat, ko želimo prevesti vse naslove v celici avtomatizacije v en naslov proizvodne mreže. Tako se naslovi pošiljateljev paketov in celice avtomatizacije zamenjajo z naslovom proizvodne mreže.

Če še vključimo funkcijo posredovanja vrat (port forwarding) pa lahko nastavimo, da se paketi na določenih vratih TCP/UDP tega naslova posredujejo udeležencu v celici avtomatizacije (npr. 10.10.1.1:81 do 192.168.10.5:80 – slika 11).



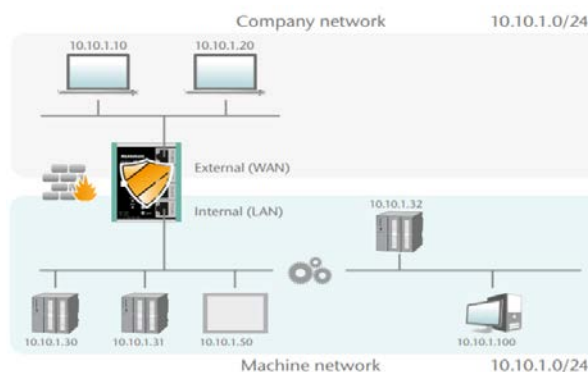
Slika 11: NAPT [3].

Če posplošimo, več stikal lahko organizira podatkovni promet med več internimi IPv4 mrežami v mrežo višjega nivoja. Tako dobijo interne mreže, računalniki in stroji enak IP naslov.

Vsako stikalo prevede IP naslov z uporabo NAT.

Tako se lahko stroje in računalnike z istim IP naslovom unikatno naslovi kar iz omrežja podjetja.

- **Posredovanje vrat:** Če stikalo uporabimo kot tako imenovani most, se bo obnašalo kot stikalo plasti 2 med celico avtomatizacije in proizvodno mrežo. Uporabimo lahko tudi paketni filter in s tem omejimo dostope med območji. Tako lahko ločimo del proizvodne mreže brez, da bi uporabili drugo mrežo.



Slika 12: Posredovanje vrat [3].

Spoznali smo nekaj osnov in primerov uporabe, vendar nikakor ne smemo pozabiti, da je PROFINET protokol fleksibilno okolje. Če danes potrebujete višje hitrosti, večje in številnejše prenose paketov in imate že zgrajeno omrežje, le-tega ni potrebno zamenjati. Zmeraj ga lahko nadgrajujete na Gigabit rešitve ali SFP povezave, pri tem pa še vedno ostajate varni pred kibernetскими napadi.

Viri:

- [1] <https://www.guru99.com/tcp-ip-model.html>
- [2] <https://profinetuniversity.com/profinet-basics/profinet-real-time-classes/>
- [3] <https://www.helmholz.de/en/>
- [4] Interni dokumenti podjetja LAPP