

IoT protokoli nivoa aplikacije

Sadržaj

- Transportni nivo
- IoT transportni servisi

Transportni nivo

Uvod

- *Transmission Control Protocol* (TCP) je konektivni transportni protokol koji nudi pouzdani prenos.
 - Kontrola protoka, kontrola zagušenja,...
 - Web, E-mail, File transfer...
- *User Datagram Protocol* (UDP) je konektivni transportni protokol koji nudi brzi prenos bez ikakvih garancija.
 - Mrežni servisi (DNS, NTP, SNMP, DHCP,...)
 - Prenos u realnom vremenu (govor, video,...)
- Prilikom izbora transportnog protokola za IoT aplikaciju moraju se sagledati zahtjevi i gornjih i donjih nivoa.
 - Većina tradicionalnih industrijskih aplikacija koriste TCP jer na nivo linka nemaju pouzdani prenos
 - TCP nije podesan za većinu ograničenih IoT uređaja i mreža

Transportni nivo

Uvod

- ❑ TCP nije efikasan za IoT aplikacije koje podrazumijevaju slanje informacija sa svega nekoliko bajta
- ❑ TCP nije podesan jer podrazumijeva neprekidno održavanje virtuelne konekcije
- ❑ Većina LLN ne može podržati veliki broj TCP sesija
- ❑ Novi IoT protokoli nivoa aplikacije, npr. *Constrained Application Protocol* (CoAP), gotovo uvijek koriste UDP pri čemu protokoli industrijskih nivoa aplikacije zahtijevaju optimizaciju i adaptaciju UDP transporta preko LLN
- ❑ Za *multicast* prenos (*upgrade firmware*) se koristi UDP.

Transportni nivo

Uvod

Device Language Message Specification/Companion Specification for Energy Metering (DLMS/COSEM)

- De facto standard u EU za daljinsko očitavanje mjerila
- Koristi TCP preko celularnih mreža a UDP preko LLN
- Povećava efikasnost smanjivanjem slanja kontrolnih informacija vezanih za uspostavljanje sesija nudeći dugotrajnu asocijaciju preko LLN.
- Za slanje velike količine podataka koriste se celularni linkovi a za manje LLN

IoT transportni servisi

Uvod

- Široka lepeza primjena IoT zahtijeva čitav spektar različitih transportnih servisa
- Česte kategorije IoT protokola nivoa aplikacije i njihovih transportnih protokola su:
 - Protokol nivoa aplikacije se ne koristi - podaci aplikacije se direktno prenose nižim protokolima
 - SCADA - razvijena mnogo prije IP ali je adaptirana za IP mreže
 - Generički „web“ protokoli (Ethernet, WiFi, 4G,...) - se koriste preko mreža bez ograničenja
 - IoT protokoli nivoa aplikacije - funkcionišu preko čvorova sa ograničenjima prilagođenim ograničenim mrežnim kapacitetima u celularnim ili satelitskim mrežama, odnosno ograničenim 6LoWPAN mrežama.
 - Message Queuing Telemetry Transport (MQTT)
 - Constrained Application Protocol (CoAP)

IoT transportni servisi

Protokol nivoa aplikacije se ne koristi

❑ Uređaji klase 0 nemaju implementiran kompletan TCP/IP stek

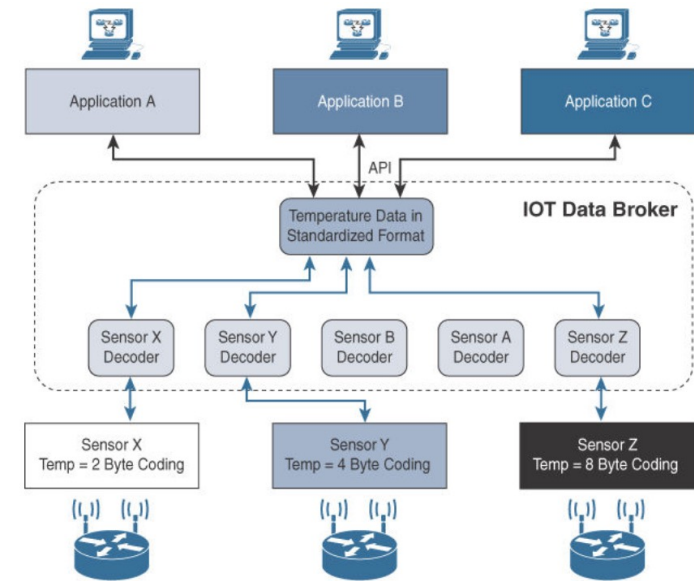
❑ Na primjer senzori temperature i vlažnosti generišu po dva bajta podataka koji se mogu

prenijeti preko LoRaWAN MAC nivoa bez korišćenja protokola TCP/IP arhitekture

❑ Metoda transportnog servisa bez protokola nivoa aplikacije nije standardizovana što otežava njenu masovnu implementaciju

❑ Korišćenje opreme različitih proizvođača generiše podatke raznorodnih formata pa je potrebna implementacija IoT Data Brokera

❑ IoT Data Broker standardizuje podatke senzora u zajednički format koji mogu koristiti autorizovane aplikacije.



David Hanes, et al, "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", Cisco Press, 2017, SAD

IoT transportni servisi

Supervisory Control and Data Acquisition (SCADA)

- ❑ Dizajnirana prije nekoliko decenija na bazi serijske komunikacije (RS-232 i RS-485) bez primjene Etherneta i IPv4
- ❑ Funkcioniše direktno na nivou linka i fizičkom nivou
- ❑ Prikuplja podatke sa udaljenih senzora pri čemu ima sposobnost da ih kontroliše
- ❑ Kontrola procesa različitih industrija u realnom vremenu
- ❑ Različiti protokoli za komunikaciju između aplikacija i uređaja
 - Modbus
 - DNP3
 - *International Electrotechnical Commission (IEC) 60870-5-101*
 - DLMS/COSEM
 - ANSI C12

IoT transportni servisi

Supervisory Control And Data Aquisition (SCADA)

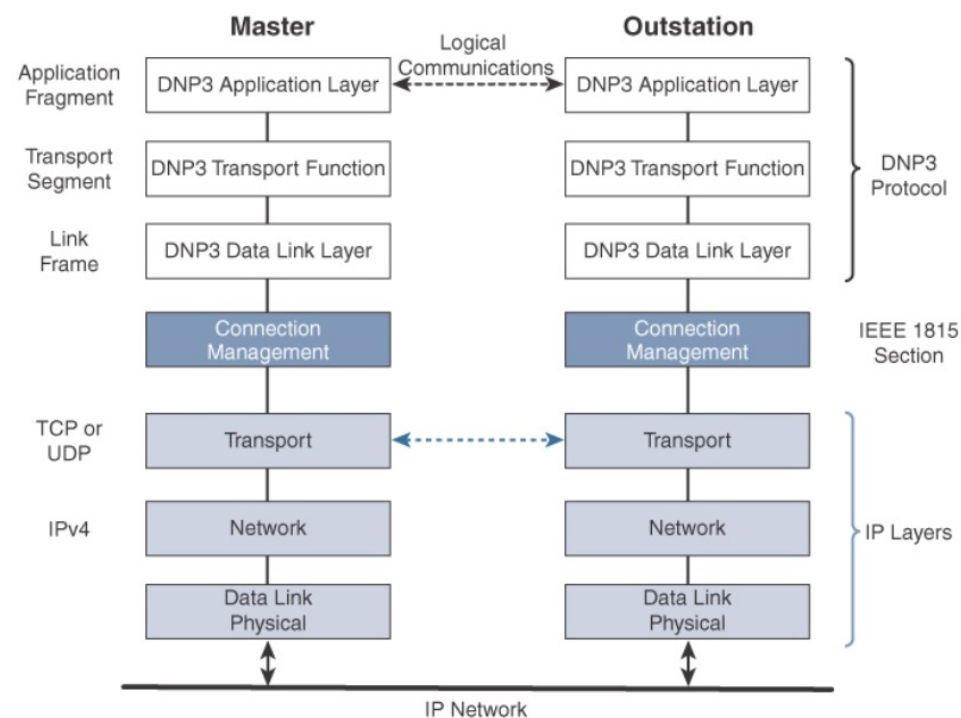
- ❑ Tokom 90-tih godina došlo je do evolucije SCADA protokola nivoa aplikacije uslijed brze implementacije Etherneta i IP
- ❑ Integracija SCADA podmreža na WAN mrežu kompanije
- ❑ Dodjela portova
 - DNP3 (IEEE 1815-2012) koristi TCP ili UDP na portu 20000 za prenos DNP3 poruka preko IP.
 - Modbus koristi TCP na portu 502.
 - IEC 60870-5-104 je unapređenje IEC 60870-5-101 za prenos preko Etherneta i IPv4 korišćenjem porta 2404 (TCP).
 - DLMS koristi IPv4 i broj porta 4059 (TCP ili UDP)

IoT transportni servisi

Supervisory Control And Data Acquisition (SCADA)

□ DNP3

- Master (server u data centru) - slave (oprema na terenu)
- Oprema na terenu prati i prikuplja podatke sa uređaja koje kontroliše
- Podaci se šalju serveru kada ih zatraži ili kada se pojave odgovarajući događaji/alarmi
- Server posjeduje kontrolne komande za upravljanje uređajima
- IEEE 1815-2012 specifikacija opisuje kako se implementacija DNP3 protokola mora adaptirati na TCP (preporuka) ili UDP.
- IP nivoi su transparentni DNP3 nivoima



David Hanes, et al, "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", Cisco Press, 2017, SAD

IoT transportni servisi

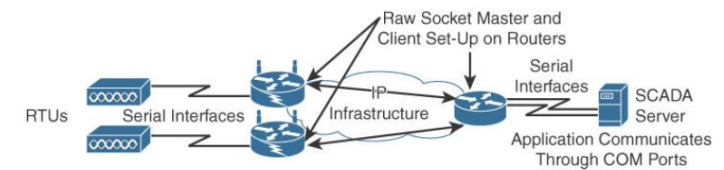
Supervisory Control And Data Acquisition (SCADA)

□ Tunelovanje

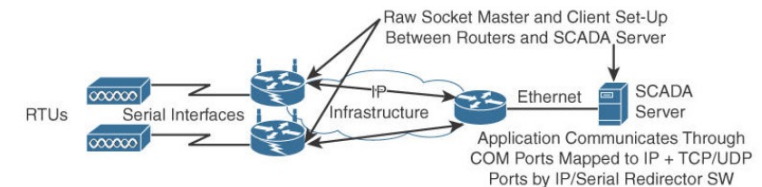
- Korišćenje *raw socket* preko TCP ili UDP
- Instaliranje uređaja koji obavljaju translacije između serijskih i IP protokola

□ *Raw socket* znači da se serijski podaci direktno prenose preko TCP ili UDP

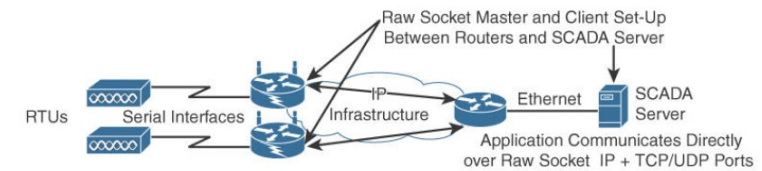
- *Raw socket* koriste novije industrijske aplikacije
- Remote Terminal Unit je višenamjenski uređaj za praćenje i kontrolu različitih sistema
- IP/serijski redirektor je softver koji terminira serijske konekcije i konvertuje ih u TCP/IP port korišćenjem *raw socket* konekcije



Scenario A: Raw Socket between Routers – no change on SCADA server



Scenario B: Raw Socket between Router and SCADA Server – no SCADA application change on server but IP/Serial Redirector software and Ethernet interface to be added



Scenario C: Raw Socket between Router and SCADA Server – SCADA application knows how to directly communicate over a Raw Socket and Ethernet interface

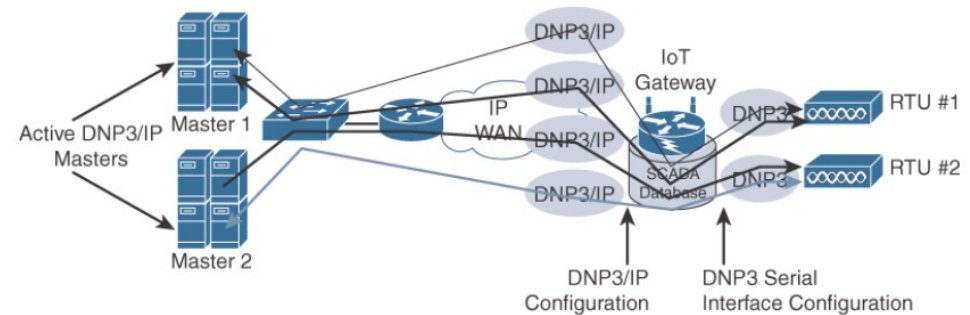
David Hanes, et al, "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", Cisco Press, 2017, SAD

IoT transportni servisi

Supervisory Control And Data Acquisition (SCADA)

□ Translacija protokola

- Prevođenje starih serijskih protokola na odgovarajuće IP verzije
- IoT gateway može obavljati funkciju translacije
- Translacija se može obavljati i direktno na IoT uređaju koji povezuje veći broj senzora



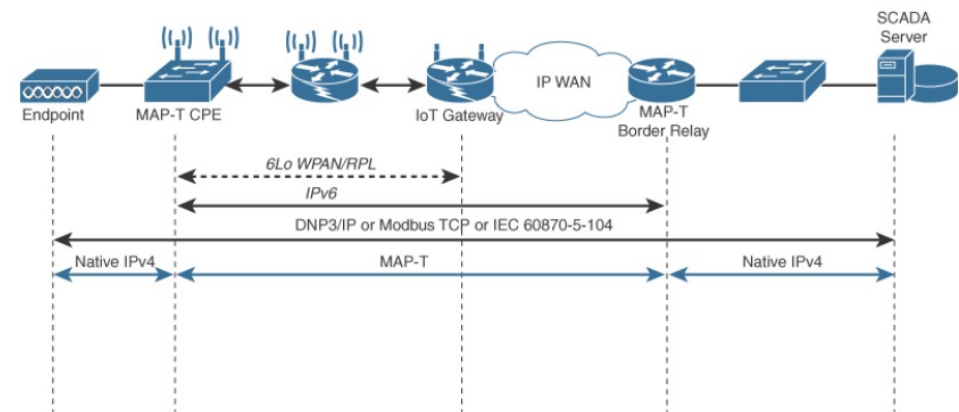
David Hanes, et al, "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", Cisco Press, 2017, SAD

IoT transportni servisi

Supervisory Control And Data Acquisition (SCADA)

□ Transport preko LLN sa MAP-T

- U ovim mrežama implementacija industrijskih protokola zahtijeva korišćenje UDP protokola
- Serveri i uređaji moraju podržavati UDP
- SCADA podržava IPv6 dok dobar dio starijih industrijskih protokola podržava samo IPv4
- Kada se koriste LLN mreže koje podržavaju samo IPv6 potreban je tranzicioni mehanizam MAP-T (*Mapping of Address and Port using Translation*, RFC 7599)
- MAP-T obavlja mapiranje IPv4 između IPv6 protokola, što omogućava da se IPv4 sobračaj prenosi preko IPv6



David Hanes, et al, "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", Cisco Press, 2017, SAD

IoT transportni servisi

Generični web bazirani protokoli

- ❑ Web bazirani protokoli su opšte prihvaćeni
- ❑ U mrežama bez ograničenja programeri mogu razvijati IoT aplikacije na sličan način kao web aplikacije (XML ili JSON podaci se mogu prenositi preko HTTP/HTTPS ili WebSocketeta)
- ❑ Web server je moguće napraviti na uređajima malih memorija
- ❑ Pažljivo treba razmotriti implementaciju klijentske ili serverske strane web aplikacije na IoT čvorištima
 - Na meteo stanici je moguće napraviti web klijenta
 - Na kameri se može napraviti web server sa malim brojem sesija
- ❑ *Extensible Messaging and Presence Protocol (XMPP)* pojednostavljuje komunikaciju između ljudi i IoT uređaja u smislu aplikacija za prenos govora, videa, chata,....

IoT transportni servisi

Generični web bazirani protokoli

- ❑ U IoT mrežama za pristup web servisima se koriste
 - *Simple Object Access Protocol (SOAP)*
 - *REpresentational State Transfer (REST)*
- ❑ SOAP (baziran na XML-u) je složen iz perspektive kodiranja, sa sporom brzinom parsiranja, ali je svestran i ima ugrađeno rukovanje greškama koje može olakšati rješavanje problema.
- ❑ XML je specifikacija koja detaljno opisuje skup pravila za kodiranje dokumenata i drugih struktura podataka na način koji je čitljiv i ljudima i računarima.
- ❑ Kao jednostavna alternativa SOAP-u, REST često implementira jednostavan URI ili JSON umjesto XML-a za zahtjeve.
- ❑ JSON je lakši za čitanje i razumijevanje od XML-a.
- ❑ REST sam po sebi nije standardno zasnovan protokol kao SOAP.

IoT transportni servisi

IoT protokoli nivoa aplikacije

- Kada se razmatraju ograničene mreže i/ili široka implementacija ograničenih čvorova, protokoli zasnovani na webu mogu biti previše izazovni za IoT aplikacije.
- IoT industrija radi na novim protokolima koji su bolje prilagođeni velikom broju ograničenih čvorova i mreža.
- Dva najpopularnija protokola su CoAP i MQTT.

CoAP	MQTT
UDP	TCP
IPv6	
6LoWPAN	
802.15.4 MAC	
802.15.4 PHY	

David Hanes, et al, "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", Cisco Press, 2017, SAD

IoT transportni servisi

IoT protokoli nivoa aplikacije

□ Constrained Application Protocol (CoAP)

- CoAP je ključni protokol nivoa aplikacije prilagođen IoT okruženju.
- IETF-ov protokol za ograničena RESTful okruženja
- IETF CoRE radna grupa (RFC 6690, RFC 7252, RFC 7641,...) blisko koordinira rad sa drugim IETF radnim grupama, posebno onima koje se bave ograničenim čvorovima i mrežama, kao što su 6Lo, 6TiSCH, LWIG, RoLL, ACE i COSE.
- CoAP u potpunosti optimizovan za IoT ograničene čvorove i mreže, dok koristi tradicionalne tehnike web programiranja kako bi bio lako razumljiv razvojnoj zajednici.
- generički okvir za aplikacije orijentisane na resurse koje ciljaju ograničene čvorove i mreže.
- CoAP definiše jednostavne i fleksibilne načine za manipulaciju sensorima i aktuatorima za upravljanje podacima ili uređajima.
- CoAP model razmjene poruka prvenstveno je dizajniran da olakša razmjenu poruka preko UDP-a između krajnjih tačaka, uključujući sigurnosni transportni protokol *Datagram Transport Layer Security* (DTLS).

IoT transportni servisi

IoT protokoli nivoa aplikacije

□ Constrained Application Protocol (CoAP)

- IETF Core radna grupa proučava alternativne mehanizme transporta, uključujući TCP, sigurnosni TLS i WebSocket.
- CoAP preko usluge kratkih poruka (SMS) kako je definisano u *Open Mobile Alliance for Lightweight Machine-to-Machine* (LWM2M) za upravljanje IoT uređajima takođe je u razmatranju
- Definisana su četiri sigurnosna načina rada:
 - NoSec,
 - PreSharedKey,
 - RawPublicKey
 - Certificate.
- Implementacije NoSec i RawPublicKey su obavezne.

IoT transportni servisi

IoT protokoli nivoa aplikacije

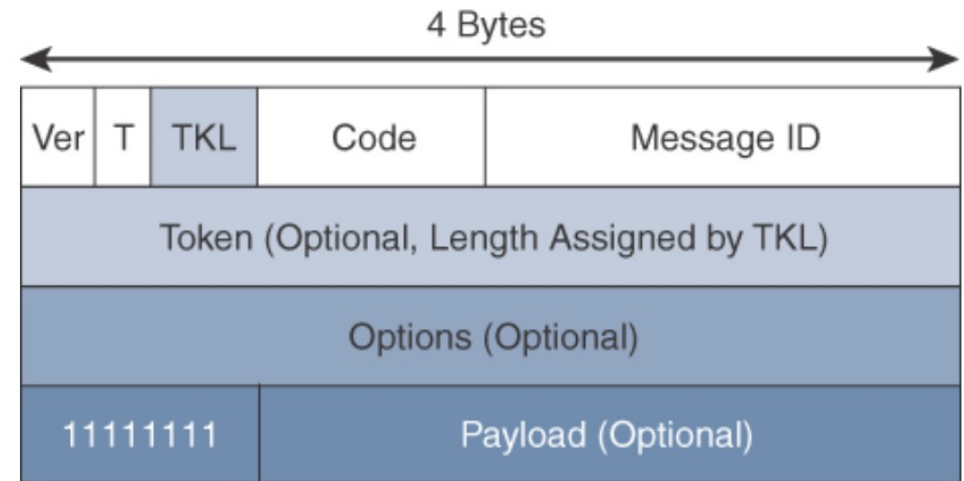
□ Constrained Application Protocol (CoAP)

○ Iz perspektive formatiranja, CoAP poruka se sastoji od

- kratkog polja zaglavlja fiksne dužine (4 bajta),
- ali obaveznog Token polja (0-8 bajtova),
- polja opcija ako je potrebno
- polja Payload.

○ Format CoAP poruke je relativno jednostavan i fleksibilan.

○ CoAP ima malo zaglavlje, što je kritično za ograničene mreže, a istovremeno ga je lako analizirati i obraditi na ograničenim uređajima.



David Hanes, et al, "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", Cisco Press, 2017, SAD

IoT transportni servisi

IoT protokoli nivoa aplikacije

□ Constrained Application Protocol (CoAP)

CoAP Message Field	Description
Ver (Version)	Identifies the CoAP version.
T (Type)	Defines one of the following four message types: Confirmable (CON), Non-confirmable (NON), Acknowledgement (ACK), or Reset (RST). CON and ACK are highlighted in more detail in Figure 6-9.
TKL (Token Length)	Specifies the size (0–8 Bytes) of the Token field.
Code	Indicates the request method for a request message and a response code for a response message. For example, in Figure 6-9, GET is the request method, and 2.05 is the response code. For a complete list of values for this field, refer to RFC 7252.
Message ID	Detects message duplication and used to match ACK and RST message types to Con and NON message types.
Token	With a length specified by TKL, correlates requests and responses.
Options	Specifies option number, length, and option value. Capabilities provided by the Options field include specifying the target resource of a request and proxy functions.
Payload	Carries the CoAP application data. This field is optional, but when it is present, a single byte of all 1s (0xFF) precedes the payload. The purpose of this byte is to delineate the end of the Options field and the beginning of Payload.

David Hanes, et al, "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", Cisco Press, 2017, SAD

IoT transportni servisi

IoT protokoli nivoa aplikacije

□ Constrained Application Protocol (CoAP)

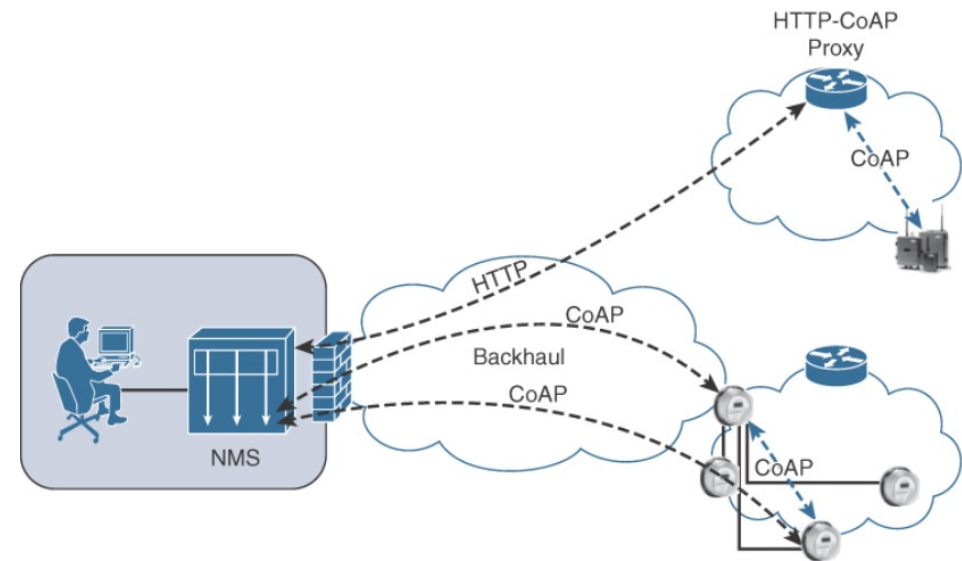
- CoAP može funkcionisati preko IPv4 ili IPv6.
- Preporučuje se da poruka stane u jedan IP paket i UDP *payload* kako bi se izbjegla fragmentacija.
- Za IPv6, sa zadanom MTU veličinom od 1280 bajtova i ne dozvoljavajući fragmentaciju među čvorovima, maksimalna veličina CoAP poruke može biti do 1152 bajta, uključujući 1024 bajta za payload.
- U slučaju IPv4, pošto se fragmentacija IP paketa može obaviti na ruterima u mreži, fragmentacije se ograničavaju postavljanjem bita IPv4 Don't Fragment (DF).
- Dok većina saobraćaja senzora i aktuatora koristi korisne sadržaje malih paketa, neki primjene, poput nadogradnje firmvera, zahtijevaju mogućnost slanja većih paketa.
- CoAP se ne oslanja na fragmentaciju IP-a, već ima svoj sopstveni sisteme prenosa informacija u više blokova.

IoT transportni servisi

IoT protokoli nivoa aplikacije

□ Constrained Application Protocol (CoAP)

- CoAP komunikacija preko IoT infrastrukture se može prenositi različitim rutama.
- Veze mogu biti između uređaja koji se nalaze na istim ili različitim ograničenim mrežama ili između uređaja i generičkih Internet ili cloud servera,
- Kompletna komunikacija ide preko IP-a.
- Proxy mehanizmi su definisani
- RFC 7252 opisuje osnovno HTTP mapiranje za CoAP.
- Kako su i HTTP i CoAP protokoli zasnovani na IP-u, proxy funkcija može biti locirana praktično bilo gdje u mreži, ne nužno na granici između ograničenih i neograničenih mreža.



David Hanes, et al, "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", Cisco Press, 2017, SAD

IoT transportni servisi

IoT protokoli nivoa aplikacije

□ *Constrained Application Protocol (CoAP)*

- Baš kao HTTP, CoAP je zasnovan na REST arhitekturi, ali sa IoT uređajem koji se ponaša i kao klijent i kao server.
- Kroz razmjenu asinhronih poruka, klijent zahtijeva akciju putem koda metode na serverskom resursu.
- *Uniform resource identifier* (URI) služi za lokalizaciju resursa na serveru.
- Server odgovara kodom odgovora koji može uključivati reprezentaciju resursa.
- Semantika CoAP zahtjeva/odgovora uključuje metode GET, POST, PUT i DELETE.
- CoAP URI format je sličan HTTP/HTTPS.
- CoAP URI šema identifikuje resurs, uključujući informacije o hostu i opcioni UDP port, kao što je naznačeno parametrima hosta i porta u URI-ju.

```
coap-URI = "coap:" "://" host [":" port] path-  
abempty ["?" query]  
coaps-URI = "coaps:" "://" host [":" port] path-  
abempty ["?" query]
```

David Hanes, et al, "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", Cisco Press, 2017, SAD

IoT transportni servisi

IoT protokoli nivoa aplikacije

□ *Constrained Application Protocol (CoAP)*

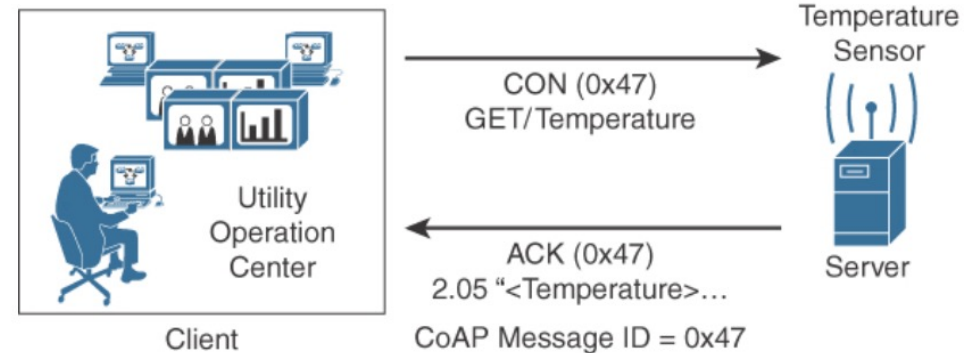
- CoAP definiše četiri tipa poruka: potvrdljive, nepotvrdljive, potvrde i reset.
- Kodovi metoda i kodovi odgovora uključeni u neke od ovih poruka čine da one nose zahtjeve ili odgovore.
- IANA je dodijelila CoAP kod, metode i kodove odgovora, brojeve opcija i format sadržaja kao parametre ograničenog RESTful okruženja (CoRE).
- Iako funkcioniše preko UDP-a, CoAP nudi pouzdan prenos poruka kada je CoAP zaglavlje označeno kao "potvrdljivo".
- CoAP podržava osnovnu kontrolu zagušenja sa zadanim time-outom, jednostavnim zaustavljanjem i čekanjem retransmisije s eksponencijalnim backoff mehanizmom i otkrivanjem duplikata poruka putem ID-a poruke.
- Ako je zahtjev ili odgovor označen kao potvrdljivi, primalac mora eksplicitno ili potvrditi ili odbiti poruku, koristeći isti ID poruke.
- Ako primalac ne može obraditi poruku koja se ne može potvrditi, šalje reset poruku.

IoT transportni servisi

IoT protokoli nivoa aplikacije

□ *Constrained Application Protocol (CoAP)*

- Operativni centar komunalnih usluga na lijevoj strani slike djeluje kao CoAP klijent, a CoAP server je temperaturni senzor na desnoj strani slike.
- Komunikacija između klijenta i servera koristi CoAP poruke čije je ID 0x47.
- CoAP ID poruke osigurava pouzdanost i koristi se za otkrivanje duplikata poruka.
- Klijent šalje GET poruku da dobije temperaturu od senzora.
- ID poruke 0x47 je prisutan za ovu GET poruku i poruka je označena sa CON.
- CON, ili potvrdljivo, u CoAP poruci znači da će poruka biti ponovo poslana sve dok primalac ne pošalje potvrdu (ili ACK) sa istim ID-om poruke.
- Senzor temperature odgovara ACK porukom koja upućuje na ispravan ID poruke 0x47.
- ACK poruka predstavlja uspješan odgovor na GET zahtjev što je označeno kodom odgovora 2.05 iza kojeg slijede traženi podaci.



David Hanes, et al, "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", Cisco Press, 2017, SAD

IoT transportni servisi

IoT protokoli nivoa aplikacije

□ *Constrained Application Protocol (CoAP)*

- CoAP podržava zahtjeve za podacima koji se šalju grupi uređaja koristeći IP Multicast.
- Implementacija IP Multicast-a sa CoAP-om zahtijeva korištenje multicast adresa za sve CoAP-čvorove.
- Za IPv4 ova adresa je 224.0.1.187, a za IPv6 je FFOX::FD.
- Ovim multicast adresama se pridružuju CoAP čvorovi koji nude usluge drugim krajnjim tačkama dok slušaju na podrazumevanom CoAP portu, 5683.
- Krajnje tačke mogu pronaći dostupne CoAP usluge putem otkrivanja multicast usluge.
- Tipičan slučaj upotrebe višestrukog slanja je implementacija nadogradnje firmvera za grupu IoT uređaja, kao što su pametni brojila.

IoT transportni servisi

IoT protokoli nivoa aplikacije

□ *Constrained Application Protocol (CoAP)*

- Pošto često nema pristupačne manuelne konfiguracije na IoT krajnjim tačkama, CoAP klijenti moraju otkriti CoAP server koji nudi usluge i resurse.
- Usluge sa CoAP servera mogu se otkriti učenjem URI-ja u imenskom prostoru ili kroz „All CoAP nodes“ multicast adresu.
- Kada se koristi URI šema za otkrivanje usluga, podrazumijevani port 5683 se koristi za nezaštićeni CoAP (coap), dok se port 5684 koristi za DTLS-obezbijeđeni CoAP (coaps).
- CoAP server mora osluškivati na ovim portovima, osim ako je drugi broj porta povezan s URI-jem u imenskom prostoru.

IoT transportni servisi

IoT protokoli nivoa aplikacije

□ *Constrained Application Protocol (CoAP)*

- Kao i kod pristupa resursima web servera, CoAP specifikacije pružaju opis odnosa između resursa u RFC 6690.
- Ovaj standard definiše format CoRE Link koji se prenosi kao payload s dodijeljenim tipom internet medija.
- Podrazumijevana ulazna tačka za izlistavanje veza resursa CoAP servera je postavljanje dobro poznatog relativnog URI-ja, kao što je /.well-known/core.
- U cilji poboljšanja vremena odgovora i smanjenja potrošnje kapaciteta mreže, CoAP podržava mogućnosti keširanja na osnovu koda odgovora.
- Da bi koristila keš unos, CoAP krajnja tačka mora potvrditi podudaranja predstavljenog zahtjeva i sačuvanog odgovora, uključujući sve opcije (osim ako nije označeno kao NoCacheKey) što potvrđuje da je sačuvani odgovor važeći.
- Dostupan je širok spektar implementacija CoAP-a, neki su objavljeni s licencama otvorenog koda, a drugi su dio rješenja proizvođača.

IoT transportni servisi

IoT protokoli nivoa aplikacije

□ *Message Queuing Telemetry Transport (MQTT)*

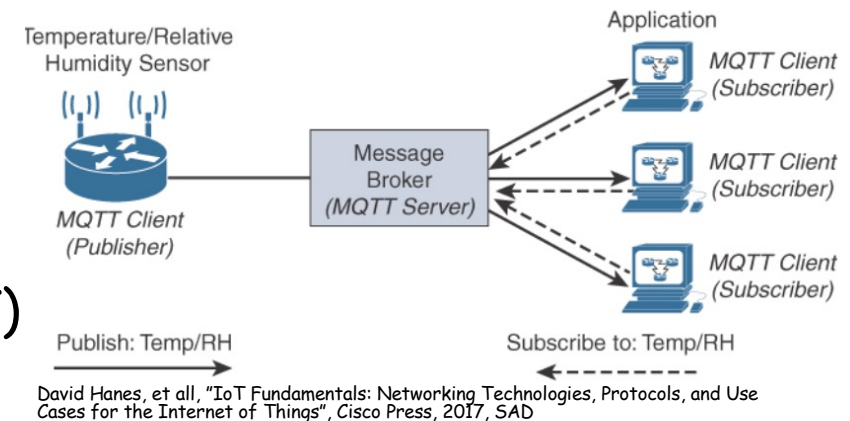
- Krajem 1990-ih, inženjeri iz IBM-a i Arcoma (koje je Eurotech kupio 2006.) tražili su pouzdan, lagan i isplativ protokol za praćenje i kontrolu velikog broja senzora i njihovih podataka sa lokacije centralnog servera, kao što se obično koristi u industriji nafte i gasa.
- Njihovo istraživanje je rezultiralo razvojem i implementacijom protokola *Message Queuing Telemetry Transport (MQTT)* koji je danas standardizovan od strane Organization for the Advancement of Structured Information Standards (OASIS).
- Uzimajući u obzir složena okruženja u industriji nafte i gasa, dizajniran je izuzetno jednostavan protokol sa samo nekoliko opcija, s obzirom na ograničene čvorove, nepouzdanu WAN *backhaul* komunikaciju i ograničenja propusnosti s promjenljivim kašnjenjima.

IoT transportni servisi

IoT protokoli nivoa aplikacije

□ Message Queuing Telemetry Transport (MQTT)

- MQTT klijent funkcioniše kao izdavač za slanje podataka (ili informacija o resursima) na MQTT server koji funkcioniše kao posrednik MQTT poruka.
- MQTT klijent na lijevoj strani slike je senzor temperature (Temp) i relativne vlažnosti (RH) koji objavljuje svoje podatke Temp/RH.
- MQTT server (ili broker poruka) prihvata mrežnu konekciju zajedno sa porukama aplikacije, kao što su podaci o Temp/RH, od izdavača.
- MQTT server upravlja procesom pretplate i odjave i prosleđuje podatke aplikacije MQTT klijentima koji djeluju kao pretplatnici.
- Aplikacija je MQTT klijent koji je pretplatnik na podatke Temp/RH koje generiše izdavač ili senzor na lijevoj strani.
- Ovaj model je sličan modelu na kojem funkcioniše Twitter.



IoT transportni servisi

IoT protokoli nivoa aplikacije

□ *Message Queuing Telemetry Transport (MQTT)*

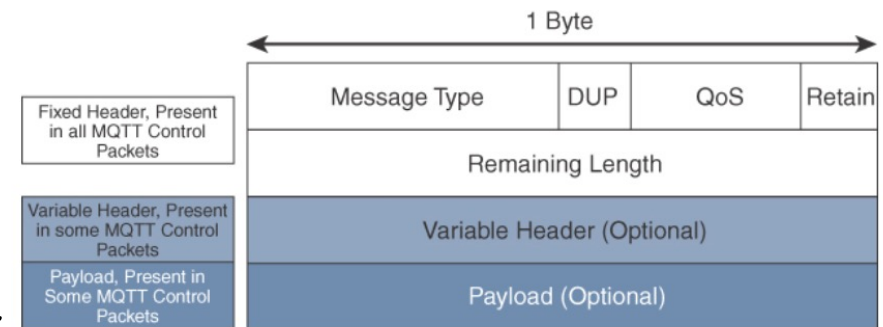
- Klijenti se mogu pretplatiti na sve podatke (koristeći wildcard) ili određene podatke izdavača.
- Prisustvo posrednika poruka u MQTT-u razdvaja prenos podataka između klijenata koji djeluju kao izdavači i pretplatnici.
- Izdavači i pretplatnici ne znaju (ili ne moraju znati) jedni za druge tako da broker MQTT poruka osigurava da informacije mogu biti baferovane i keširane u slučaju kvarova na mreži.
- Izdavači i pretplatnici ne moraju biti online istovremeno.
- MQTT kontrolni paketi se prenose preko TCP transporta koristeći port 1883.
- TCP osigurava uređeni tok bajtova bez gubitaka između MQTT klijenta i MQTT servera.
- MQTT se može opciono osigurati korišćenjem TLS-a na portu 8883, a može koristiti i WebSocket.
- MQTT je jednostavni protokol jer se svaki kontrolni paket sastoji od 2-bajtnog fiksnog zaglavlja s opcionim varijabilnim poljima zaglavlja i opcionim korisnim opterećenjem.
- Treba imati na umu da kontrolni paket može sadržati do 256 MB.

IoT transportni servisi

IoT protokoli nivoa aplikacije

□ *Message Queuing Telemetry Transport (MQTT)*

- U poređenju sa formatom CoAP poruke, može se vidjeti da MQTT sadrži manje zaglavlje od 2 bajta u poređenju sa 4 bajta za CoAP.
- Prvo MQTT polje u zaglavlju je Message Type, koje identifikuje vrstu MQTT paketa unutar poruke.
- U MQTT verziji 3.1.1 specificirano je četrnaest različitih tipova kontrolnih paketa, pri čemu svaki od njih ima jedinstvenu vrijednost koja je kodirana u polje Vrsta poruke.
- Vrijednosti 0 i 15 su rezervisane.



David Hanes, et al, "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", Cisco Press, 2017, SAD

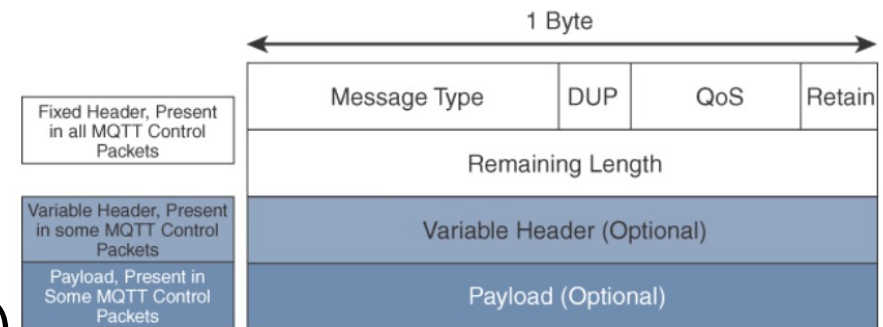
Message Type	Value	Flow	Description
CONNECT	1	Client to server	Request to connect
CONNACK	2	Server to client	Connect acknowledgement
PUBLISH	3	Client to server Server to client	Publish message
PUBACK	4	Client to server Server to client	Publish acknowledgement
PUBREC	5	Client to server Server to client	Publish received
PUBREL	6	Client to server Server to client	Publish release
PUBCOMP	7	Client to server Server to client	Publish complete
SUBSCRIBE	8	Client to server	Subscribe request
SUBACK	9	Server to client	Subscribe acknowledgement
UNSUBSCRIBE	10	Client to server	Unsubscribe request
UNSUBACK	11	Server to client	Unsubscribe acknowledgement
PINGREQ	12	Client to server	Ping request
PINGRESP	13	Server to client	Ping response
DISCONNECT	14	Client to server	Client disconnecting

IoT transportni servisi

IoT protokoli nivoa aplikacije

□ *Message Queuing Telemetry Transport (MQTT)*

- Sljedeće polje u zaglavlju MQTT je DUP (Duplication Flag). Ova zastavica, kada je postavljena, omogućava klijentu da zabilježi da je paket prethodno poslan, ali potvrda nije primljena.
- Polje zaglavlja QoS omogućava izbor tri različita QoS nivoa.
- Retain flag se nalazi samo u PUBLISH poruci, i služi za obavještanje servera da zadrži podatke poruke što omogućava novim korisnicima da odmah dobiju posljednju poznatu vrijednost bez čekanja na sljedeće ažuriranje od izdavača.
- Posljednje obavezno polje u zaglavlju MQTT poruke je Remaining length koje specificira broj bajtova u MQTT paketu koji slijedi nakon ovog polja.
- MQTT sesije između svakog klijenta i servera sastoje se od četiri faze: uspostavljanje sesije, autentifikacija, razmjena podataka i završetak sesije.
- Svaki klijent koji se povezuje sa serverom ima jedinstveni ID klijenta, koji omogućava identifikaciju MQTT sesije između obje strane.
- Kada server isporučuje poruku aplikacije više od jednom klijentu, svaki klijent se tretira nezavisno.



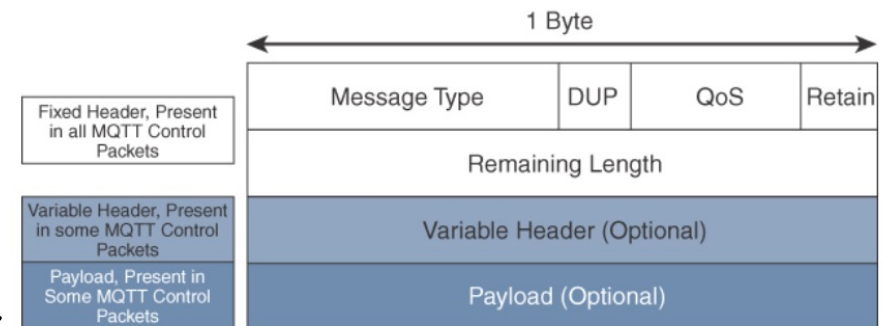
David Hanes, et al, "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", Cisco Press, 2017, SAD

IoT transportni servisi

IoT protokoli nivoa aplikacije

□ *Message Queuing Telemetry Transport* (MQTT)

- Pretplate na resurse generišu SUBSCRIBE/SUBACK kontrolni paketi, dok se odjava vrši kroz razmjenu UNSUBSCRIBE/UNSUBACK kontrolnih paketa.
- Prekid veze se vrši preko kontrolnog paketa DISCONNECT, koji takođe nudi mogućnost klijentu da se ponovo poveže tako što ponovo pošalje svoj ID klijenta da bi nastavio sa komunikacijom.
- Broker koristi *topic string* ili *topic name* za filtriranje poruka za svoje pretplatnike.
- Nakon pretplate na resurs, *subscriber* ukazuje na jedan ili više nivoa *topic*-a koji se koriste za strukturiranje naziva *topic*-a.



David Hanes, et al, "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", Cisco Press, 2017, SAD

Message Type	Value	Flow	Description
CONNECT	1	Client to server	Request to connect
CONNACK	2	Server to client	Connect acknowledgement
PUBLISH	3	Client to server Server to client	Publish message
PUBACK	4	Client to server Server to client	Publish acknowledgement
PUBREC	5	Client to server Server to client	Publish received
PUBREL	6	Client to server Server to client	Publish release
PUBCOMP	7	Client to server Server to client	Publish complete
SUBSCRIBE	8	Client to server	Subscribe request
SUBACK	9	Server to client	Subscribe acknowledgement
UNSUBSCRIBE	10	Client to server	Unsubscribe request
UNSUBACK	11	Server to client	Unsubscribe acknowledgement
PINGREQ	12	Client to server	Ping request
PINGRESP	13	Server to client	Ping response
DISCONNECT	14	Client to server	Client disconnecting

IoT transportni servisi

IoT protokoli nivoa aplikacije

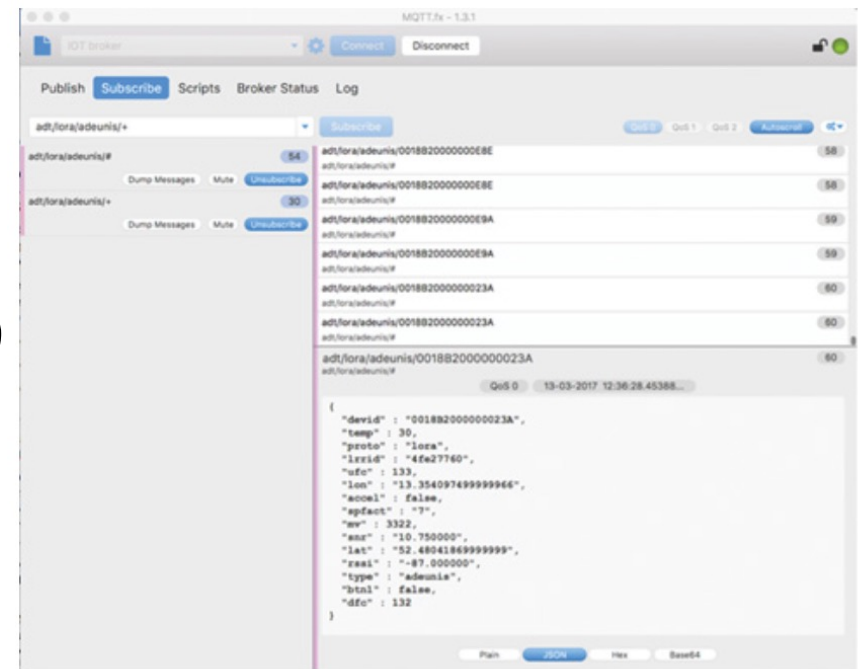
□ *Message Queuing Telemetry Transport (MQTT)*

- Kosa crta (/) u nazivu MQTT *topic*-a se koristi za odvajanje svakog nivoa unutar stabla *topic*-a i pružanje hijerarhijske strukture nazivima *topic*-a.

- Slika ilustruje ove koncepte sa `adt/lora.adeunis` kao nivoom *topic*-a i

- `adt/lora/adeunis/0018B2000000023A` kao primjerom naziva *topic*-a.

- Široka fleksibilnost dostupna je klijentima koji se pretplate na naziv *topic*-a.
- Može se pretplatiti na jedan *topic* ili se može pretplatiti na više *topic*-a odjednom, korišćenjem zamjenskih znakova.
- Pretplata može sadržati jedan od zamjenskih znakova kako bi se omogućila pretplata na više *topic*-a odjednom.



David Hanes, et al, "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", Cisco Press, 2017, SAD

IoT transportni servisi

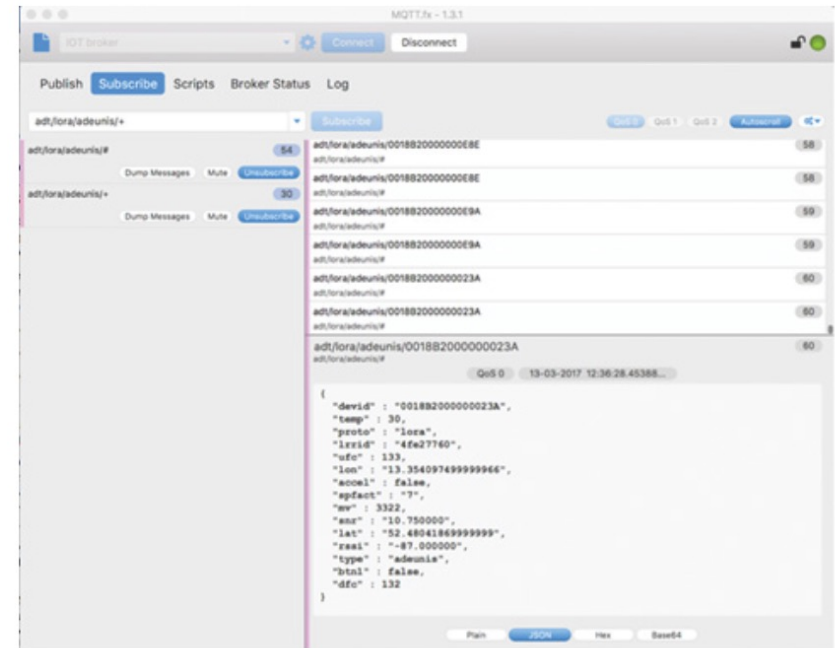
IoT protokoli nivoa aplikacije

□ *Message Queuing Telemetry Transport (MQTT)*

- Znak funte (#) je zamjenski znak koji odgovara bilo kojem broju nivoa unutar *topic*-a.
- Zamjenski znak na više nivoa predstavlja roditeljski i bilo koji broj podređenih nivoa.
- Na primjer, pretplata na `adt/lora/adeunis/#`

omogućava prijem cijelog podstabla, koje može uključivati nazive *topic*-a kao što su:

- `adt/lora/adeunis/0018B20000000E9E`
- `adt/lora/adeunis/0018B20000000E8E`
- `adt/lora/adeunis/0018B20000000E9A`



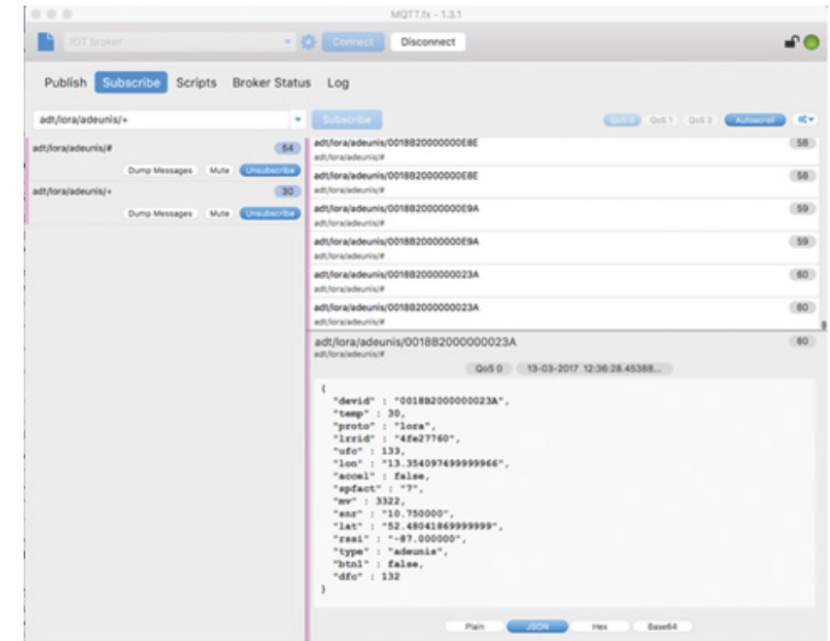
David Hanes, et al, "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", Cisco Press, 2017, SAD

IoT transportni servisi

IoT protokoli nivoa aplikacije

❑ *Message Queuing Telemetry Transport (MQTT)*

- Znak plus (+) je zamjenski znak koji odgovara samo jednom nivou *topic*-a.
- Na primjer, `adt/lora/+` dozvoljava pristup `adt/lora/adeunis/` i `adt/lora/abeway`, ali ne i `adt/lora/adeunis/0018B20000000E9E`.
- Nazive *topic*-a koji počinju znakom dolara (\$) server mora isključiti kada pretplate počinju sa zamjenskim znakovima (# ili +).
- Često se ove vrste naziva *topic*-a koriste za internu statistiku brokera poruka, tako da klijenti ne mogu objavljivati poruke na ove *topic*-e.
- Na primjer, pretplata na `+/monitor/Temp` ne prima nijednu poruku objavljenu na `$SYS/monitor/Temp`. Ovaj *topic* bi mogao biti kontrolni kanal za neki temperaturni senzor.



David Hanes, et al, "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", Cisco Press, 2017, SAD

IoT transportni servisi

IoT protokoli nivoa aplikacije

□ Message Queuing Telemetry Transport (MQTT)

- PINGREQ/PINGRESP kontrolni paketi se koriste za validaciju veza između klijenta i servera.
- Slično ICMP pingovima koji su dio IP-a, oni pomažu u održavanju i provjeri TCP sesije.
- Osiguravanje MQTT veza putem TLS-a je opcija jer zahtijeva više resursa na ograničenim čvorovima.
- Kada se TLS ne koristi, klijent šalje korisničko ime i lozinku u običnom tekstu tokom pokretanja veze.
- Implementacije MQTT servera takođe mogu prihvatiti anonimne klijentske konekcije (sa korisničkim imenom/lozinkom koja je „prazna“).
- Kada se implementira TLS, klijent mora potvrditi sertifikat servera za ispravnu autentifikaciju.
- Provjera autentičnosti klijenta takođe se može izvršiti putem razmjene sertifikata sa serverom, zavisno od konfiguracije servera.

IoT transportni servisi

IoT protokoli nivoa aplikacije

□ Message Queuing Telemetry Transport (MQTT)

- MQTT protokol nudi tri nivoa kvaliteta usluge (QoS).
- QoS za MQTT se implementira prilikom razmjene poruka aplikacije sa publisher-a ili subscriber-a, i razlikuje se od IP QoS-a.
- Protokol isporuke je simetričan.
- Klijent i server mogu preuzeti ulogu publisher-a ili subscriber-a.
- Protokol slanja se bavi isključivo slanjem poruke aplikacije od jednog pošiljaoca do jednog primaoca.

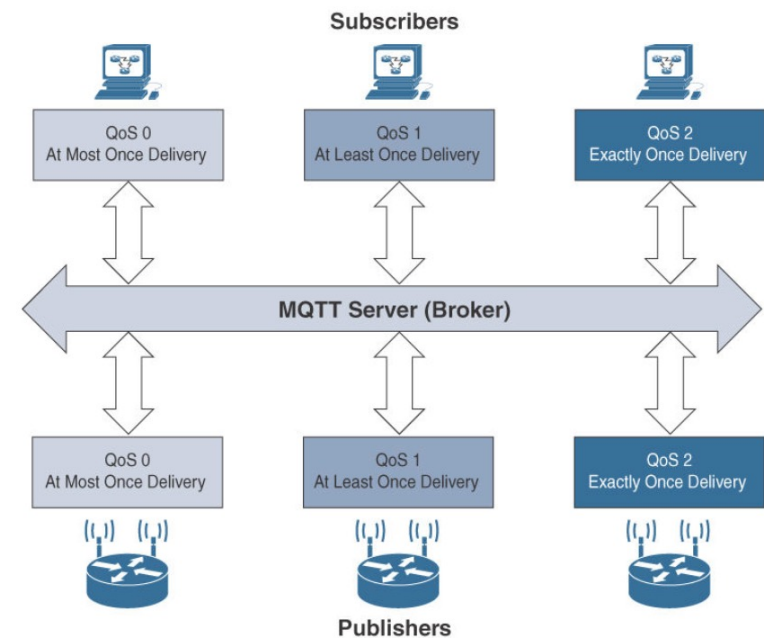
IoT transportni servisi

IoT protokoli nivoa aplikacije

□ Message Queuing Telemetry Transport (MQTT)

○ Tri nivoa MQTT QoS-a:

- QoS 0: Ovo je najbolja i nepotvrđujuća usluga podataka koja se naziva isporuka „najviše jednom“. Publisher šalje svoju poruku jednom serveru, koji je jednom šalje pretplatnicima. Primaoc ne šalje odgovor, a pošiljalac ne obavlja retransmisiju. Poruka primaocu stiže ili jednom ili nikako.
- QoS 1: Ovaj QoS nivo osigurava da se slanje poruke između publishera i servera, a zatim između servera i subscribera-a dogodi barem jednom. U PUBLISH i PUBACK paketima, identifikator paketa je uključen u zaglavlje varijable. Ako poruka nije potvrđena PUBACK paketom, šalje se ponovo. Ovaj nivo garantuje isporuku „barem jednom“.
- QoS 2: Ovo je najviši nivo QoS-a, koji se koristi kada ni gubitak ni duplikat poruka nijesu prihvatljivi. Povećano je zaglavlje za ovaj QoS nivo jer svaki paket sadrži opciono varijabilno zaglavlje s identifikatorom paketa. Potvrda prijema PUBLISH poruke zahtijeva proces potvrde u dva koraka. Prvi korak se obavlja preko para paketa PUBLISH/PUBREC, a drugi se postiže parom paketa PUBREL/PUBCOMP. Ovaj nivo pruža „zagarantovanu uslugu“ poznatu kao dostava „tačno jednom“, bez obzira na broj retransmisija sve dok se poruka jednom ne isporuči.



David Hanes, et al, "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", Cisco Press, 2017, SAD

IoT transportni servisi

IoT protokoli nivoa aplikacije

□ Message Queuing Telemetry Transport (MQTT)

Factor	CoAP	MQTT
Main transport protocol	UDP	TCP
Typical messaging	Request/response	Publish/subscribe
Effectiveness in LLNs	Excellent	Low/fair (Implementations pairing UDP with MQTT are better for LLNs.)
Security	DTLS	SSL/TLS
Communication model	One-to-one	many-to-many
Strengths	Lightweight and fast, with low overhead, and suitable for constrained networks; uses a RESTful model that is easy to code to; easy to parse and process for constrained devices; support for multicasting; asynchronous and synchronous messages	TCP and multiple QoS options provide robust communications; simple management and scalability using a broker architecture
Weaknesses	Not as reliable as TCP-based MQTT, so the application must ensure reliability.	Higher overhead for constrained devices and networks; TCP connections can drain low-power devices; no multicasting support

David Hanes, et al, "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", Cisco Press, 2017, SAD