МОНГОЛ УЛСЫН ШИНЖЛЭХ УХААН ТЕХНОЛОГИЙН ИХ СУРГУУЛЬ
МЭДЭЭЛЭЛ, ХОЛБООНЫ ТЕХНОЛОГИЙН СУРГУУЛЬ

Чулуунцэцэг Төгсжаргал

B140970113

SDN сүлжээний топологи илрүүлэх протоколуудын харьцуулсан судалгаа

Мэргэжил: Системийн аюулгүй байдал

Систем хамгааллын төсөл

Улаанбаатар хот

2017 он

Гарчиг

Зургийн жагсаалт

Бүлэг 1

Ерөнхий хэсэг

1.1 Зорилго

Энэхүү төслийн ажлаар SDN сүлжээний топологи илрүүлэх протоколуудын харьцуулсан судалгаа хийх. Mininet симуляцын програм ашиглан SDN сүлжээний протоколуудын харьцуулсан график гаргана. SDN сүлжээг зохион байгуулснаар сүлжээний администны ажлыг хөнгөвчилснөөр цаг хугацаа болон эдийн засагт хэмнэлт гаргана.

1.2 Зорилт

Энэхүү төслийн зорилт нь бол SDN сүлжээний ажиллагаа болон төхөөрөмжүүдийг хэрхэн удирдахыг судлан симуляцын програм дээр туршиж үзэх байгаа. Сүлжээний админ нь Controller ашиглан тухайн байгууллагынхаа бүх төхөөрөмж рүү хандан алсаас хандан удирдах цаашлаад тохиргооны файлыг гарган авч OpenFlow протокол ашиглан төхөөрөмж рүүгээ дамжуулах боломжтой юм.

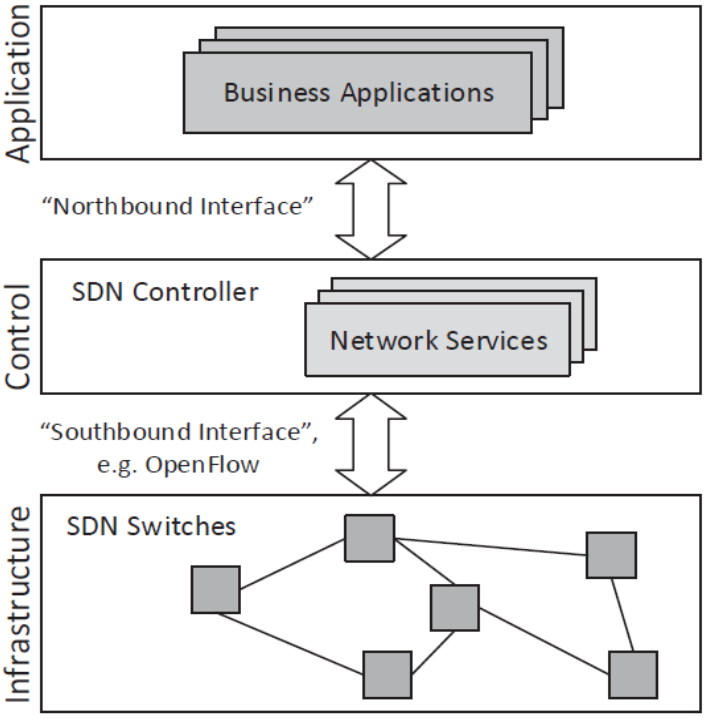
Бүлэг 2

Онолын хэсэг

2.1 SDN сүлжээ

Software-Defined network буюу програм хангамжаар тодорхойлогдсон сүлжээ гэдэг нь төвлөрсөн эсвэл тархсан платформ дахь удирдлагын функцуудыг төвлөрүүлэх зорилгоор өгөгдөл дамжуулах үе шатнаас удирдлагын үе шатыг салгасан нээлттэй стандартад суурилсан сүлжээ юм. SDN сүлжээ нь өндөр түвшний програмчлалын хэл болон интерфейсүүд ашиглан том хэмжээний сүлжээг автоматаар болон динамикаар удирдахыг сүлжээний администраторт зөвшөөрдөг фреймворк юм. SDN сүлжээ нь шууд програмчлах боломжтой, хурдан ажиллагаатай, төвлөрсөн удирдлагатай, тохиргоо програмчлагдсан, үйлдвэрлэгч болон борлуулагчийн төхөөрөмжүүд өөр хоорондоо харшихгүй давуу талуудтай. Мөн төвлөрсөн удирдлагатай учраас сүлжээ хариуцагч болон сүлжээний инженерийн ажлыг хөнгөвчилж, ажиллагааны хувьд ч илүү хурдан, найдвартай. Уламжлалт IP сүлжээний хувьд рутер нь пакетыг дамжуулахаас (өгөгдлийн хэсэг) гадна замчлалын протоколыг ажиллуулан сүлжээний замыг олж илрүүлэх, замчлалын шийдвэрийг гаргах (хяналт удирдлагын хэсэг) гэсэн үйл ажиллагааг зэрэг хийдэг бол SDN нь үүнээс өөр юм. SDN-ын хувьд рутер, свитч зэрэг дамжуулах, холбох төхөөрөмжүүдийн ухаалгаар удирдах үүрэг нь тэдгээрээс хасагдаж, үүний оронд эдгээр үйл ажиллагаа нь SDN контроллер гэж нэрлэгдэх логик нэгжид төвлөрдөг байна. Үүнийг програм хангамжид хэрэгжүүлдэг. SDN-ыг хэрэгжүүлснээр сүлжээг програмчлах боломж нэмэгдэхийн зэрэгцээ технологийн шинэчлэл инновацийг нэвтрүүлэх боломжтой болно. Контроллер дээр ажиллаж байгаа програм хангамжийг ашиглан сүлжээний шинэ үйлчилгээнүүд, аппликэйшн, policy буюу бодлого зэргийг хялбархан хэрэгжүүлж

болдог. Контроллерын програм хангамж нь сайн тохируулсан API-аар дамжуулах элементүүдийг (өгөгдлийн хэсэг) удирдана, жишээлбэл OpenFlow. Тохирох дүрмүүдийг суулгаж өгснөөр, контроллерын программ нь SDN-ын свитчүүдийг замчлах (routing), холбох (switching), хамгаалалт хийх (firewalling), сүлжээний хаягийн хөрвүүлэлт хийх (NAT), ачаалал тэнцвэржүүлэх (load balancing) зэрэг өргөн хүрээний үйл ажиллагааг гүйцэтгэх боломжтой болгож програмчилж чадна.



Зураг 2.1: SDN бүтэц

SDN технологи нь :

- Удирдлагын үе шат болон өгөгдөл дамжуулах үе шатыг салгасан. Сүлжээний төхөөрөмжөөс удирдлагын үе шатыг (програм хангамж) салгаснаар сүлжээний төхөөрөмж энгийн нэг өгөгдөл дамжуулах төхөөрөмж болсон.
- Нэгэн ижил эх үүсгэвэрийн хаяг болон хүлээн авах хаяг бүхий пакетуудын дарааллыг нэг флов (урсгал) гэдэг. Өгөгдөл дамжуулах төхөөрөмжүүд фловын эхний пакетийг дамжуулсан төлөвийн мэдээллийг хадгалж авдаг ба энэ төлөвийн дагуу дараагийн пакетуудыг боловсруулдаг. Өмнө нь өгөгдлийг дамжуулах үйл

ажиллагаа нь зөвхөн хүрэх хаягууд дээр тулгуурлаж хийгддэг байсан бол одоо пакетын олон талбарууд дээр үндэслэгдэж дамжуулалт хийгддэг болсон. Тиймээс сүлжээний төхөөрөмжүүдийг рутер, свитч, галт хана гэж ялгах шаардлагагүй болсон.

- Удирдлагын үе шат нь сүлжээний үйлдлийн систем (Network Operating System) буюу SDN контроллер луу шилжсэн. Сүлжээний үйлдлийн систем нь өгөгдөл дамжуулах төхөөрөмжүүдийг нэгдсэн логик удирдлагатай болгож байгаа сервер дээр суусан програм хангамж юм. Үүний зорилго нь уламжлалт сүлжээний үйлдлийн системтэй ижил юм.

- Өгөгдөл дамжуулах төхөөрөмжтэй шууд холбогддог. NOS дээр ажиллаж байгаа програм хангамжаар сүлжээ програмчлагддаг.

2.1.1 SDN сүлжээний үндсэн 3 түвшин

Аппликейшн түвшин (Application layer)

SDN загварын хамгийн дээд түвшин нь аппликэйшн түвшин юм. Сүлжээний дээд түвшний бодлого, шийдвэрүүд энд тодорхойлогдож, хэрэгжинэ.
Аппликэйшн түвшин болон удирдлагын түвшний хоорондын интерфэйсийг Northbound **(хойш чиглэлт холболт)** гэж нэрлэдэг.
Удирдлагын түвшин болон дэд бүтцийн түвшний хоорондын интерфэйсийг Southbound **(урагш чиглэлт холболт)** гэж нэрлэдэг. Сүлжээнд траффик анализ болон хяналт хийдэг OpenFlow, NetFlow гэх мэт протоколуудыг ашигладаг.

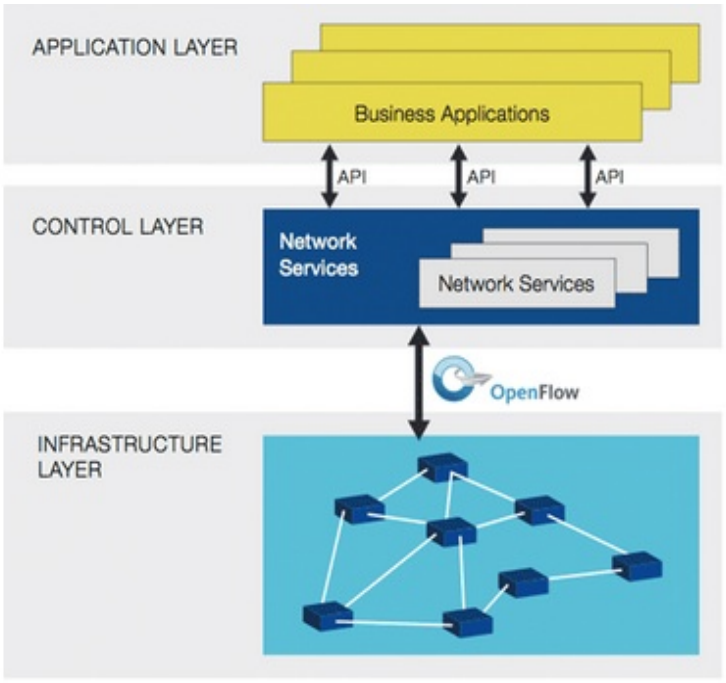
Удирдлагын түвшин (Control layer)

Удирдлагын түвшин нь дэд бүтцийн түвшин буюу сүлжээний төхөөрөмжүүдийг удирдах бөгөөд сүлжээний бүх тохиргоо болон бодлогын удирдлагыг зохицуулдаг төвлөрсөн нэг буюу хэд хэдэн контроллероос бүрддэг. Контроллерын нэг чухал үүрэг нь сүлжээний ерөнхий дүрслэлийг харуулах явдал юм.

Дэд бүтцийн түвшин (Infrastructure layer)

Дэд бүтцийн түвшинд өгөгдлийн үйл ажиллагаагаар хангах үүрэг бүхий SDN свитчүүд буюу хоорондоо харилцан холбогдсон дамжуулах элементүүдээс бүрдсэн дэд бүтцийн давхаргыг харуулж байна. Эдгээр свитчүүд нь техник тоног төхөөрөмж байж болохоос гадна, программ хангамжид суурилсан, мөн Open vSwitch гэх мэт виртуал

свитч байж болно.



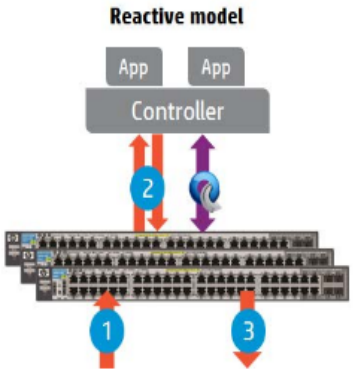
Зураг 2.2: SDN сүлжээний 3 түвшин

2.1.2 SDN сүлжээний урсгал зохицуулалт

SDN сүлжээ нь Реактив болон Проактив гэсэн хоёр аргаар флов буюу урсгалыг зохицуулдаг.

Реактив арга

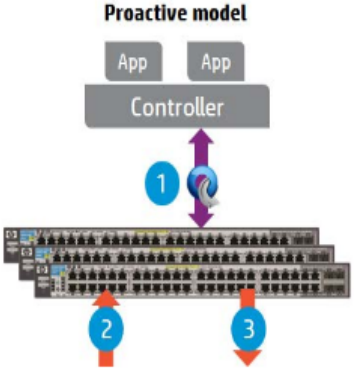
Эхний пакет свичд ирэх үед, свич пакетийг хэрхэн удирдахаа мэддэггүй. Тиймээс свич пакетийг контроллер руу илгээдэг. Контроллер офенплов протокол ашиглан свичийн флов хүснэгт рүү фловыг оруулах үүрэгтэй. Энэ аргын гол дутагдалтай тал нь свич нь контроллерын шийдвэрээс бүрэн хамааралтай учраас свич контроллертой холболт тасарвал пакетыг удирдаж болохгүй болох юм.



Зураг 2.3: Reactive бүтэц

Проактив арга

Контроллер нь свич тус бүрийн флов хүснэгтэнд флов оруулгыг урьдаас тооцоолдог. Энэ арга нь reactive аргаас илүү давуу талтай бөгөөд хэрвээ свич контроллертой холболт тасарвал траффик алдагдахгүй. Уламжлалт аргаас илүү SDN сүлжээний гол давуу тал нь бодит сүлжээнд шинэ аппликейшнийг хурдан тестлэх, хөгжүүлэх, ажиллагааны болон капиталын зардлыг хэмнэх, мөн свич тус бүрийн менежментийг төвлөрүүлсэнд оршино.



Зураг 2.4: Proactive бүтэц

2.1.3 SDN сүлжээгээр дамжигдах мессэжүүд

Ямар ч сүлжээний хувьд сүлжээний төхөөрөмжүүд танилт хийхийн тулд хоорондоо мессэж солилцдог.

Свич хоорондын мессэж (controller-to-switch)

Handshake болон багцын гаралт (packet-out) төрлийн мессэжүүд нь флов оролтыг суулгадаг. Мөн свичийн тохиргоо, тохиргооны үүрэг, асинхрон мессэжийн тохиргоог засварлах гэх мэт маш олон тохиргоог удирддаг. Энэ мессэжүүд нь свич болон контроллёр хооронд TCP холболт үүсгэн контроллероос свич рүү дамжуулагддаг.

Асинхрон мессэж (asynchronous)

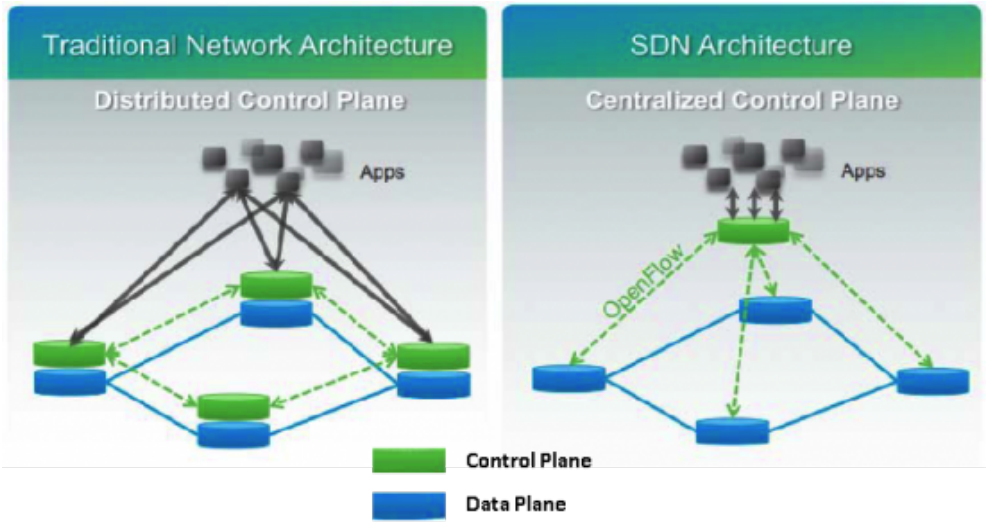
Энэ мессэжүүд нь урсгал алдагдах, устгагдах, порт статус болон алдааны мессэж гэсэн шалтгаантайгаар контроллер луу илгээгддэг багцын оролтын (packet-in) төрлийн мессэж.

Симметрик мессэж (symmetric)

Энэ төрлийн мессэжүүд нь hello, echo request, echo replay, болон experimenter гэх мэт handshake хийх зорилготойгоор ашиглагддаг. Энэ мессэж нь свич болон контроллерын альнаас нь ч хүсэлт илгээгүй байхад илгээгддэг.

2.1.4 SDN сүлжээний давуу тал :

- Боловсруулалтын хоцролтыг багасгаснаар хурдан ажиллагаатай болсон
- Сүлжээг шууд програмчлах боломжтой
- Тохиргоо програмчлагдсан
- Төвлөрсөн нэг удирдлагатай
- Харилцагч болон сүлжээний инженерийн ажлыг хөнгөвчилсөн
- Ажиллагаа илүү найдвартай
- Үйлдвэрлэгч болон борлуулагчийн төхөөрөмжүүд өөр хоорондоо харшихгүй
- Нээлттэй стандарт



Зураг 2.5: Уламжлалт болон SDN сүлжээний бүтэц

2.1.5 SDN сүлжээний контроллерууд

Контроллер нь өгөгдөл дамжуулах төхөөрөмжүүдийг удирдаж чигийг заадаг. Маш олон төрлийн контроллерууд байдаг. Эдгээр нь дэмжих буюу таних програмын хэл, ажиллагаа гэх мэт шинж чанаруудаасаа ялгаатай байдаг. Ерөнхийдөө контроллерын гол зорилго нь сүлжээний төхөөрөмжид урсгалын дүрэм нэмэх юм. Өгөгдлийг пакет замчлалын мэдээллийн бааз (Routing Information Base) гэж нэрлэгддэг бөгөөд энд сүлжээний топологи хадгалагддаг. Замчлалын мэдээллийн баазыг ихэнхдээ сүлжээн дэх контроллерууд бусад тохиолдолд хоорондоо мэдээлэл солилцох замаар байнга хадгалагдаж байдаг. Флов хүснэгтийн оруултууд нь ихэвчлэн дамжуулах мэдээллийн бааз (Forwarding Information Base) гэж нэрлэгддэг бөгөөд энэ нь ихэвчлэн жирийн төхөөрөмжийн удирдлагын болон өгөгдлийн үе шат хооронд толин тусгал хэлбэрээр байдаг.

SDN Controllers

- Floodlight
- HP VAN SDN
- NOX
- OpenDaylight
- POX

2.2 Ерөнхий хэсэг

2.2.1 LLDP протокол

Link Layer Discovery Protocol (LLDP)-г 2005 онд анх IEEE-ээс IEEE 802.1AB нэртэйгээр стандарчилж гаргасан. 2009 онд энэхүү нормыг хүчин төгөлдөр болгож, албан ёсоор 802.1AB IEEE-2009 хэмээн баримтжуулсан IEEE стандартад заасан "Станц ба Хэвлэл Мэдээллийн Хэрэгслийн Хандалтыг Удирдах Холболтыг Илрүүлэх" протокол гэж шинэчилсэн хувилбарыг стандартчилсан. LLDP нь нэг хандалтаар хөршийн мэдээллийг илрүүлэх протокол юм, өөрөөр хэлбэл тухайн сүлжээний мөн чанар болон чадамжийг харуулж, зэргэлдээ орших свичүүдээс ижил мэдээллийг хүлээн авдаг. Цаашилбал энэ нь OSI загварын layer-2-д ажилладаг вендоруудаас гаргасан олон тооны протоколуул дээр тулгуурласан илрүүлэх /discovery/ протокол юм. (Жишээ нь: Cisco Discovery Protocol (CDP), Nortel Discovery Protocol (NDP), Extreme Discovery Protocol (EDP) гэх мэт) ОпенФловд суурилсан сүлжээнүүд дээр топологи илрүүлэхэд ашигладаг LLDP протоколын хамгийн чухал онцлогуудын талаар дурьдвал. LLDP фрейм бүр нь **Зураг 2.6-т** үзүүлсэн шиг (LLDPDU) буюу ачааллаж байгаа LLDP өгөгдлийн хэсэг болон толгойн хэсгээс бүрддэг. LLDP мессэж бүрийн толгойн хэсэгт нь Ethertype хэсгийн анхдагч утга нь 0x88cc гэж байдаг бөгөөд энэхүү мэдээлэл нь ОпенФлов сүлжээнүүд дэх илрүүлэх пакетуудыг үр дүнтэй тодорхойлоход маш чухал ач холбогдолтой байдаг. DestinationMAC нь multicastDestinationMAC-н хаягийн олонлог юм. Энэхүү хаягийг "LLDP multicastaddress" гэж стандартаар нэрлэдэг бөгөөд энэ нь уламжлалт свичүүдэд LLDP илрүүлэх пакетуудыг тодорхойлох боломж олгодог. LLDPDU нь нэмэлт болон заавал байх ёстой Type Length Value (TLV) бүтцүүдээс бүрддэг. Заавал байх ёстой гурван TLV-ээр ачааллаж эхлээд, араас нь хэд хэдэн нэмэлт TLV-г ажиллуулж, төрөл ба уртын талбар нь 0 байх ёстой тусгай TLV-ээр дуусдаг. Нэмэлт TLV-д нь TLV-н Суурь ба Зохион байгуулалттай Тусгай TLV-үүд багтдаг бөгөөд тэдгээрийг LLDP протоколоор дамжуулан илрүүлэх шинэ онцлогуудыг гаргаж ирэхэд ашиглах боломжтой.

Preamble	Destination MAC	Source MAC	Ethertype	Chassis ID TLV	Port ID TLV	Time to live TLV	Optional TLVs	End of LLDPDU TLV	Frame check sequence
	01:80:c2:00:00:0e, or 01:80:c2:00:00:03, or 01:80:c2:00:00:00	Station's address	0x88CC	Type=1	Type=2	Type=3	Zero or more complete TLVs	Type=0, Length=0	

Зураг 2.6: LLDP Ethernet Frame Structure

Илрүүлэх протоколын үйл ажиллагааны хүрээнд гол цөмийг бий болгодог үндсэн дөрвөн TLV байдаг.

- Chassis ID - Энэхүү TLV нь LLDP пакет илгээсэн свичийг тодорхойлно.
- Port ID - Энэхүү TLV нь LLDP пакет илгээсэн портын мэдээлэл байна.
- Time to Live - Энэхүү TLV нь нэгж хугацаанд боломжит LLDP пакет хүлээн авсан мэдээлэл.
- End of LLDPDU - LLDP фреймийн ачааллын төгсгөлийг тодорхойлох тусгай TLV юм.

TLV type	TLV name	Usage in LLDPPDU
0	End of LLDPDU	Mandatory
1	Chassis ID	Mandatory
2	Port ID	Mandatory
3	Time To Live	Mandatory
4	Port description	Optional
5	System name	Optional
6	System description	Optional
7	System capabilities	Optional
8	Management address	Optional
9–126	Reserved	-
127	Custom TLVs	Optional

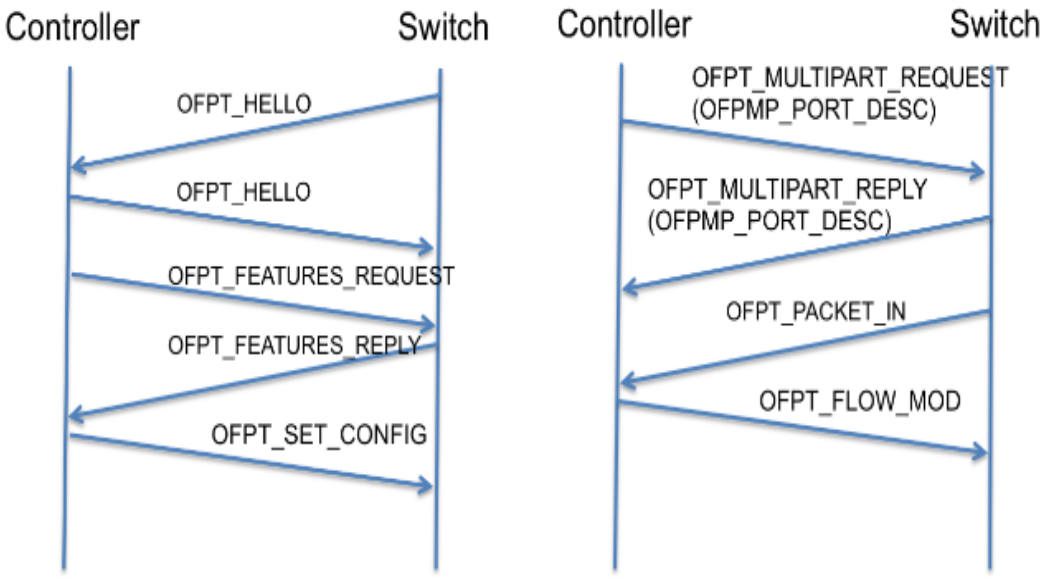
Зураг 2.7: TLV Type Values

Уламжлалт сүлжээнд тогтмол хугацаанд свичүүдийн LLDP фрейм илгээх функцыг сүлжээний администраторууд тохируулдаг. Харин ОпенФловд суурилсан сүлжээнүүдийн хувьд свич нь LLDP мессэжийг контроллерын хүсэлтээр үндсэн топологийг илрүүлэхээр илгээдэг.

2.2.2 OPENFLOW

OpenFlow гэдэг нь удирдлагын түвшин (control layer) ба дэд бүтцийн түвшний (infrastructure layer) хоорондын интерфэйс болох southbound (өмнө зүгт чиглэсэн) интерфэйст зориулсан стандарт протокол юм. Практик дээр бол OpenFlow нь SDN контроллер болон SDN свитчүүдийн хоорондын холболтын интерфэйсийг хангадаг ба ингэснээр свитчүүдийг тохируулах, удирдах боломжийг контроллерт олгодог байна. OpenFlow-ыг идэвхжүүлсэн SDN свитчийг өөрийнх нь контроллерын IP хаяг болон TCP портын дугаараар тохируулсан байна. Тухайн свитч нь асах үедээ тохиргооныхоо дагуу харгалзах IP хаяг болон TCP порт дээр өөрийн контроллертай холбогдох ба холболтын аюулгүй байдлыг хангах зорилгоор Transport Layer Security (TLS) холболтыг үүсгэнэ. Протокол анхны холболтоо тогтоох үед, контроллер нь OpenFlow-ын OFPT_FEATURES_REQUEST мессэжийг ашиглан тохиргооны мэдээллийг свитчээс авна. Энэ мэдээлэлд тухайн свитчний идэвхитэй портууд (сүлжээний интерфэйсүүд) болон түүнд харгалзах MAC хаягууд орно. Свитч-Контроллерын анхны холболт тогтоох (handshake) үйл ажиллагаа нь тухайн сүлжээнд байгаа node буюу свитчүүдийн талаар мэдээллийг контроллерт мэдээлэх боловч, тухайн сүлжээнд байгаа свитчүүдийн хооронд байж болох боломжит холболтын талаар мэдээлдэггүй тул топологийн дүрслэлийг бүрэн гаргах боломжгүй байдаг. OpenFlow нь SDN свитчүүдийн дамжуулалтын дүрмүүдэд (forwarding rule) хандалт хийж, удирдах боломжийг контроллерт олгох ба ингэснээр контроллер нь сүлжээгээр урсгалыг хэрхэн дамжуулахыг удирдах юм. OpenFlow-тай зохицож ажиллах свитч нь match-action буюу нийцүүлэн-үйлдэл хийх системийг дэмждэг байх хэрэгтэй. Энэхүү match-action системийн үүрэг нь ирж байгаа пакет бүрийг урьдчилан тохируулсан дүрмүүдэд нийцэж байгаа эсэхийг шалгах ба тохирох дүрмийн дагуу үйлдлүүдийг гүйцэтгэдэг юм. OpenFlow свитчний хийдэг нэгэн чухал үйлдэл нь пакетыг свитчний тодорхой нэг порт руу дамжуулах эсвэл тухайн пакетыг устгах үйлдэл хийдэг. Дамжуулах дүрэмд (forwarding rule) тодорхойлогдсон свитчийн портууд нь физик портуудаас бүрдэх ба мөн үүнээс гадна виртуал портуудыг агуулдаг байна. Үүнд: ALL (бүх физик портуу-

даар пакетыг илгээнэ), CONTROLLER (OpenFlow-ын Packet-In мессэжээр SDN контроллер руу илгээнэ), FLOOD (ALL-тай адил боловч орж ирсэн ingress портыг хасна). OpenFlow нь мөн үүнээс гадна олон үйлдлийг дэмждэг ба тэдгээрээс дурьдвал, пакетын толгой мэдээллийг дарж бичих, TTL талбарыг шинэчлэх, VLAN болон MPLS tag-уудыг нэмэх, устгах, эх үүсвэрийн болон очих MAC хаягийг дахин бичих гэх мэт. Свитч нь өөрийн аль ч портоороо хүлээж авсан дата пакетыг контроллер руу дамжуулна. Үүнийг OpenFlow Packet-In мессэжээр OFPT_PACKET_IN хийдэг. Жишээлбэл, свитч нь дамжуулах дүрмийн алинд ч нийцэхгүй пакетыг хүлээж авсан үедээ үүнийг ашиглана. Энэ тохиолдолд свитч нь пакетыг OpenFlow-ын Packet-In мессэжинд багтаан контроллер руу дамжуулдаг. Үүнийг хүлээж авсан контроллер нь тухайн шинэ урсгалд харгалзах дамжууллын дүрмийг суулгах эсэхээ шийддэг байна.



Зураг 2.8: SDN мессэжний бүтэц

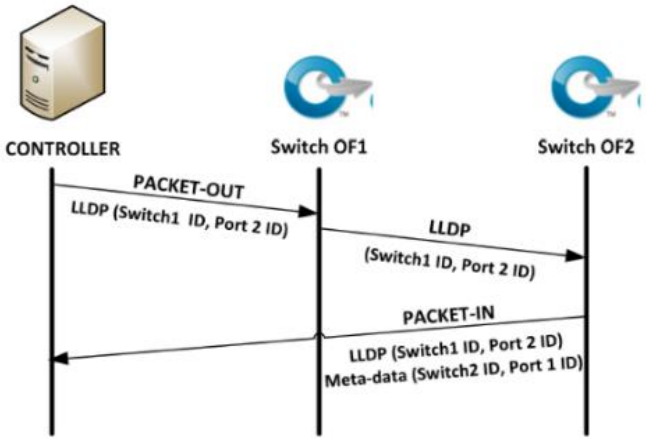
2.3 Нэг домэйнт сүлжээнд топологи илрүүлэх

Удирдлагын нэг домэйнд топологи илрүүлэх процессыг дан ганц ОФ свичээс бүрдсэн сүлжээнд эсвэл уламжлалт болон ОпенФлов свичээс бүрдсэн холимог сүлжээнд гүйцэтгэх боломжтой.

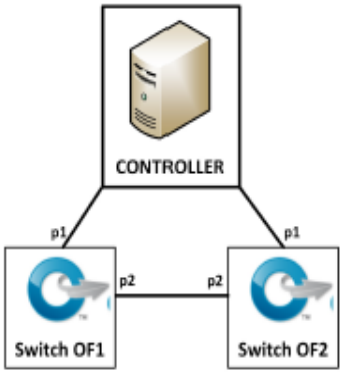
2.3.1 Зөвхөн ОпенФлов свичтэй сүлжээ

ОпенФлов сүлжээ нь свич хоорондын холболтуудыг илрүүлэхдээ нэг хоп хөрш илрүүлэх LLDP протоколыг ашиглана. Дан ганц ОпенФловын төхөөрөмжүүдээс бүрдсэн сүлжээн дэх холболтуудыг илрүүлэхдээ ямар нэг өөр илрүүлэх техник хэрэггүй. Учир нь топологи илрүүлэх аргыг дэмждэг свич холболт бүрийн төгсгөлд байрладаг. ОпенФлов техникийн тодорхойлолтуудыг агуулдаг свичүүд нь топологийг илрүүлэх боломжтой болгохын тулд үндсэн хоёр тохиргоо байдаг. Эхлээд мастер контроллерын IP хаяг болон TCP портын олонлог ОФ свич бүрт байдаг бөгөөд төхөөрөмжийг асаангуут холболт үүсгэхийн тулд контроллеруудын IP хаягнууд ажилладаг. Хоёрдугаарт свичүүд нь контроллерын өөр өөр портуудаар хүлээн авсан EtherType нь 0x88cc байх Packet-In мессэжээр дамжуулан контроллерт замчлалын чиглэлийг дахин тодорхойлдог. Свич ажиллаж эхлэхэд сүлжээндэх контроллерыг хайж, тохиргооны мессэж, урсгалын хүснэгт гэх мэт мэдээллүүдийг илгээж, хүлээн авахын тулд TLS (TransportLayer Security) протоколоор дамжуулан аюулгүй шифрлэгдсэн холболт үүсгэхийг оролдож байдаг. Анхны мэдээлэл солилцох хэсэг болох контроллер нь свичэд (FEATURE REQUEST MESSAGE) мессэж илгээдэг ба свичээс (FEATURE REPLY MESSAGE) хариу мессэж илгээдэг. Эдгээр мессэжээр Свич ID, MAC, идэвхитэй портын жагсаалт гэх мэт холболтуудыг илрүүлэх параметрүүдийн мэдээллийг контроллерт илгээдэг. Үүгээр контроллер ОпенФлов свичүүд хоорондоо холбогдсон гэдгийг мэддэг бөгөөд холболтыг илрүүлэхэд маш хэрэгцээтэй ойлголтуудыг хүлээн авдаг. Энэхүү мессэжээр гарч ирсэн мэдээлэл дээр тулгуурлан контроллер удирдлагын домэйнд хамааралтай ОпенФлов свичүүдэд идэвхитэй байгаа портын тоог мэдэж авдаг. Контроллер нь Packet-Out мессэжийг тухайн сүлжээнд илрүүлсэн свич дээрх идэвхитэй порт бүрт өгдөг бөгөөд эдгээр мессэжд нь LLDP пакетыг агуулдаг. Packet-Out мессэж нь мөн LLDP пакетийн ашигтай ачааллын TLV талбарт заасан портоор LLDP бүрийг замчлахын тулд харгалзах мессэжийн нэвтрэлтийг свичэд өгнө. ОпенФлов свич нь контроллерийн илгээсэн LLDP мессэжийг хүлээн авахдаа, тухайн мессэжийг зэргэлдээх свичрүү тохирох Порт ID (TLV)-ээр явуулдаг. Свич OF1 ба Свич OF2-ын хоорондын холболтыг илрүүлэхийн тулд контроллер болон ОпенФлов свичүүдийн хооронд нэг чиглэлд солилцсон мессэжүүдийг Зураг 5-ын диаграмд харуулав. Үүний адилаар, энэхүү зурвас солилцох нь эсрэг чиглэлд ч мөн адил байна. Тэдгээр Packet-In-ийг хүлээн авсны дараа, контроллер нь LLDPDU-т агуулагдах мэдээлэл болон мета-өгөгдөлд цуглуулсан өгөгдлүүдэд тулгуурлан хоёр ОпенФлов свичийн

хоорондын холболтыг илрүүлэх боломжтой болдог.Контроллер нь энэ мэдээллийг мэдээллийн баазад хадгалах ба улмаар сүлжээний топологийн статусийг шинэчилж байдаг. Топологи илрүүлэх процесс нь бүхэлдээ стандарт утга 5 секундын default утгатай тодорхой хугацаанд давтана.



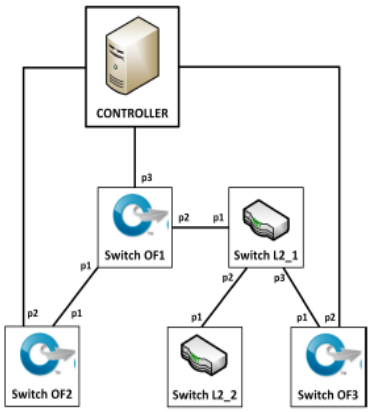
Зураг 2.9: LLDP-д суурилсан топологийг илрүүлэх



Зураг 2.10: Нэг домайнт ОпенФлов свич дээр суурилсан сүлжээ

2.3.2 Уламжлалт ба Опенфлов Свичтэй Сүлжээ

Холимог Опенфлов домэйний ОФ свичийг илрүүлэх механизм нь дээр дурдсанаас ялгаагүй. ОпенФлов свичтэй анх мессэж солилцлох үед контроллер нь түүний байршил болон чадамжийг илрүүлдэг.Уламжлалт свичтэй тохиолдолд, контроллер нь эдгээр свичүүдийг илрүүлэх боломжгүй, учир нь тэдний хооронд ямар ч мессэж солилцдоггүй юм. Уламжлалт свичтэй холимог Опенфлов сүлжээнд, Опенфлов-г дэмждэг свичүүдийн хооронд үндсэндээ холболтын хоёр төрөл байдаг.



Зураг 2.11: Нэг домайнт Уламжлалт болон ОпенФлов свич дээр суурилсан сүлжээ

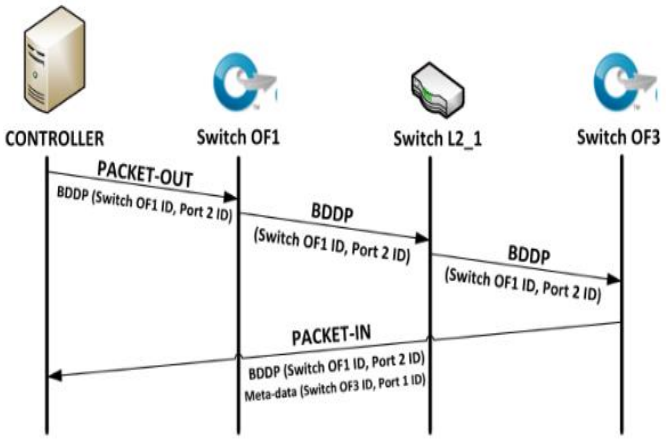
- OF свич хоорондын шууд холболт. Энэ холболт нь Зураг **2.11-т** үзүүлсэн, свич OF1 порт p1 болон свич OF2 порт p2 гэсэн OF свичийн идэвхтэй хоёр порт дундах шууд холболт юм.

- Уламжлалт свичүүдтэй үед Опенфлов свичүүд хоорондын холболт. Энэ нь Опенфлов свичын Опенфлов 1 порт p2 болон свич Опенфлов3 порт p1 гэсэн идэвхтэй хоёр порт хоорондын шууд-бус холболтыг хэлэх боловч эдгээр нь **2.11-т** үзүүлсний дагуу, ижил домэйнд байсан хэвээр байгаа юм.

Одоогоор, уламжлалт болон ОФ свичээс бүрдсэн сүлжээний холболтонд илрүүлэлт хийхийн тулд үндсэн ОпенСорс контроллеруудын зарим нь LLDP ба BDDP (Broadcast Domain Discovery Protocol) layer-2-ын топологийг илрүүлэх протоколуудын хослолыг ашигладаг. BDDP протокол гэдэг нь холимог Опенфлов сүлжээний олон хоп холбол-

тыг илрүүлэхэд, Floodlight ба OpenDayLight (ODL) гэх мэт Опенсорс контроллерт программчлагдсан өвөрмөц шийдэл юм. BDDP мессэж нь LLDP пакеттай ижил бүтцийг харуулдаг ба дээрх хэсэгт үзүүлсний дагуу зайлшгүй болон нэмэлт TLV бүтцээс бүрдсэн фрем юм. Гол ялгаа нь фремийн толгойн destinationMAC хаягын талбарт байгаа юм. Энэ талбар нь LLDP протоколын ашигласан multicast хаягын оронд (ff:ff:ff:ff:ff:ff) broadcast хаягтай болдог. Энэ онцлог нь уламжлалт свичүүдийг нэг хоптой илрүүлэх протоколын асуудлыг хаяглах замаар BBDP пакетийг явуулах боломжийг олгодог. Энэ аргаар, олон хоптой холболтыг ОФ свичийнхтэй адил broadcast домэйнд хамаарах уламжлалт свичүүдийг ашиглан илрүүлэх боломжтой. Өөр нэгэн том ялгаа нь BDDP толгойн дах EtherType талбар юм. Энэ протокол нь LLDP мессэжнд ашиглагдсанаас өөр утга ашигладаг. Ерөнхийдөө 0x8999 гэдэг нь BDDP фремд ашигласан утга юм. Уламжлалт свичээр шууд бус холболтыг илрүүлэхийн тулд, контроллер нь свич бүрийн идэвхтэй порт бүрээр сүлжээнд илгээгдэх нэг Packet-Out дотор нэг BDDP мессэжийгбагцалдаг. Packet-Out-ыг илгээснээр, мессэжийг хүлээн авч буй ОФ свичүүдийн мэдээллийг тодорхойлдог. BDDP пакетийг боловсруулсны дараа, ОФ свич нь мессэжийг TLV талбар (Порт ID)-т заасан портоор хөрш свичэд явуулдаг. Энэ пакетад свич (Свич ID, Порт ID г.м)-ийг таних LLDP-ынхтэй ижил параметрүүд ордог. Хөрш свич нь Опенфлов эсвэл уламжлалт свичийг дэмждэг төхөөрөмж байх боломжтой. Эхний тохиолдолд, пакет нь мессэжийн Ethertype 0x8999-тэй дамжуулалт хийх ба үүнийг шууд контроллерлуу Packet-In-ээр илгээнэ. Хөрш нь уламжлалт свич байх тохиолдолд, энэ нь пакетын destinationMAC хаягыг шалгана. Ингэснээр, энэ нь broadcast хаяг (ff:ff:ff:ff:ff:ff) болохыг мэдэх бөгөөд пакетыг бүх портуудаараа дамжуулна. Хөршийнх нь ядаж нэг нь Опенфловыг дэмждэг гэж үзвэл, энэ нь контроллерт Packet-In-ээр мессэж илгээнэ. Энэхүү Packet-In мессэжнд мета-өгөгдөл багтсан байгаа бөгөөд эцэст нь олон хоптой холболтыг илрүүлэхэд шаардагдах мэдээллийг контроллерт өгч байдаг. Энэ аргачлалыг гүйцэтгэсний дараа домэйн контроллер нь 2 ОФ свичүүдийн хоорондын шууд бус холболтыг илрүүлэхэд шаардагдах мэдээлэл бүхий Packet-In-ээр хүлээн авсан BDDP пакеттай болно. Свич ОФ1 ба Свич ОФ3-ын хоорондын шууд бус холболтыг илрүүлэхийн тулд контроллер ба ОФ свичүүдийн хооронд нэг талдаа солилцсон мессэжүүдийг харуулсан байна. Хэдийгээр холимог Опенфлов сүлжээний BDDP протоколийн хэрэглээ нь суурь топологийн ОФ свичүүд хоорондын олон хоптой холбоог илрүүлэх үр дүнтэй шийдэл байж болох боловч, үүнд зарим нэг аргачлалууд бий. BDDP нь Floodlight ба

ODL гэх мэт хэд хэдэн Опенсорс контроллерийн эх кодод програмчлагдсан топологийг илрүүлэх тусгай шийдэл юм.



Зураг 2.12: BDDP-д суурилсан топологийг илрүүлэх