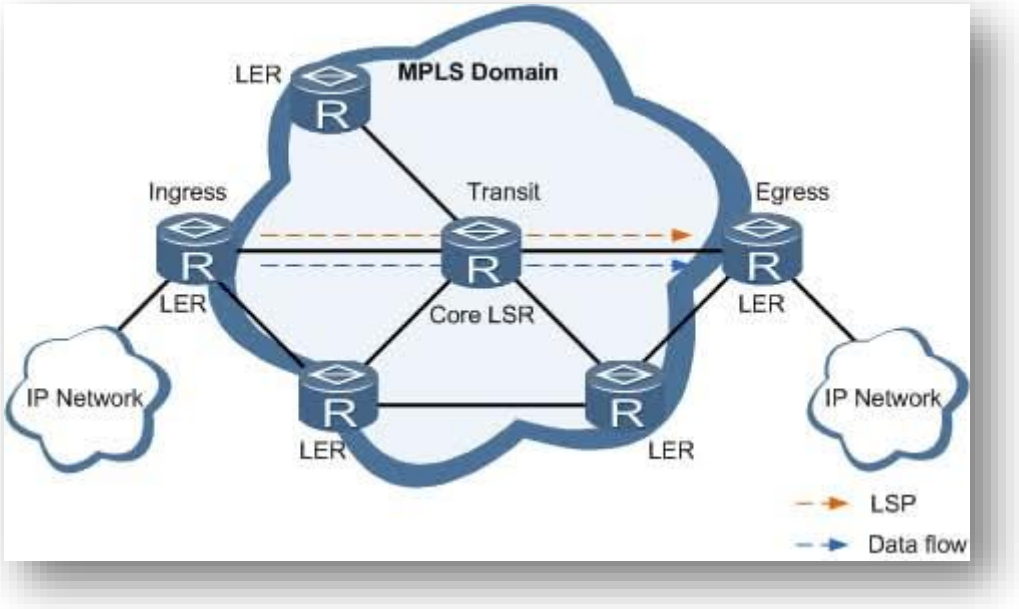
Multiprotocol Label Switching (MPLS)

What is MPLS?

Multiprotocol Label Switching (MPLS) ဆိုတာကတော့ Circuit Switching ၊ Packet Switching တို့လိုပဲ Switching Technique တစ်ခုဖြစ်ပြီးတော့ Label Switching Technique တစ်ခုဖြစ်ပါတယ်။ 1998 ခုနှစ်မှာ Internet Engineering Task Force (ITEF) ကနေ Developed လုပ်ခဲ့ပါတယ်။ Service Provider တွေမှာအသုံးများကြပါတယ်။ Label Switching ကို မသွားခင်မှာ ပုံမှန် Packet Switching တစ်ခုဘယ်လိုအလုပ်လုပ်သလဲ အရင်ကြည့်ရအောင်။ Source ကနေ Destination ကို Data Packet တစ်ခုပို့တယ် ဆိုပါစို့။ Packet ထဲမှာ Source IP ပါမယ်၊ Destination IP ပါမယ်။ Router တစ်ခုကိုဖြတ်တဲ့အခါမှာ Packet ကိုဖွင့်မယ်၊ Destination IP ကိုဖတ်မယ်၊ ဆိုင်ရာဆိုင်ရာ ကို Forward လုပ်မယ်၊ ဒါမျိုးပေါ့။ Destination ကိုမရောက်မချင်း Router တွေအကုန်လုံးက ဒီ Process ကိုပဲလုပ်ကြပါတယ်။ ပြောရရင် Layer 3 Address အထိဖောက်ဖတ်ရတယ်ပေါ့။ နှေးတယ်ပေါ့။ Label Switching မှာ Label က 20-bit ရှိပြီးတော့ Layer 2 Header နဲ့ Layer 3 Header ကြားမှာနေရာယူပါတယ်။ ဒါကြောင့် MPLS ကို Layer 2.5 လို့ခေါ်ကြတာပေါ့။ Label Switching မှာက ပထမဆုံး FEC ကို အရင်သတ်မှတ်ပါတယ်။ FEC ဆိုတာက Forwarding Equivalence Class ၊ IP Packet တွေကို သဘောတရား တူရာတူရာစုပြီး ခွဲလိုက်တဲ့သဘောပေါ့။ ပြီးရင် LSR (Label Switching Router) တွေအချင်း ဘယ် FEC ဆိုရင်တော့ ဘယ် Label ကပ်ဆိုပြီး Agree လုပ်ကြတာကိုတော့ Label Binding လို့ခေါ်ပါတယ်။ အဲ့ဒီမှာလဲ IP Packet တစ်ခုအတွက် LSR အချင်းချင်း Swap လုပ်တဲ့ Label တွေက လမ်းကြောင်းတစ်လျှောက်လုံး တူနေမှာမဟုတ်ပါဘူး။ ဒါကတော့ LSR တွေရဲ့ Label Binding သဘောအရသွားမှာပါပဲ။ အဲ့ဒီ LSR Label Binding ကိုတော့ LDP (Label Distribution Protocol) က လုပ်သွားမှာဖြစ်ပါတယ်။ IP Packet တစ်ခုကို LER (Label Edge Router) မှာ Label စကပ်တာကို **"Push"** ၊ LSR အချင်းချင်း Label Exchange လုပ်တာကို **"Swap"** ၊ LER မှာ Label ကို ခွာချပြီး Traditional IP Packet အနေနဲ့ ပို့လိုက်တာကို **"Pop"** လုပ်တယ်လို့ခေါ်ပါတယ်။ အဲ့ဒီတော့ Labeled Packet ကိုခဏနေကလို ပို့ကြည့်ရအောင်။ Source ကနေ ပထမဆုံး LER ကို IP Packet ဝင်လာမယ်။ ပုံမှန်အတိုင်းပဲ Source IP ၊ Destination IP ပါမယ်ပေါ့။ အဲ့ဒီမှာ LER က ဝင်လာတဲ့ Packet တွေကိုဖတ်ပါတယ်။ သူ့ရဲ့ဆိုင်ရာဆိုင်ရာ FEC အလိုက် Pre-determined Path တွေအတိုင်း Label Push လုပ်ပြီး Forward လုပ်ပါတယ်။ အဲ့ဒီမှာ LSR တွေက ခဏနေကလို Destination IP အထိမဖတ်တော့ပါဘူး။ Destination က ဘာဆိုတာကိုလဲစိတ်မဝင်စားတော့ပါဘူး။ Label တွေကိုဖတ်ပါတယ်။ သူ့ရဲ့ LDP Label Binding အရ ဆိုင်ရာဆိုင်ရာ FEC အလိုက် Label တွေကို Swap လုပ်ပြီး Forward လုပ်ပါတယ်။ ဒီလိုပုံစံနဲ့ပဲ Destination ရောက်အောင် Forward လုပ်ပါတယ်။ ပြောရရင် မြန်တယ်ပေါ့။ Label ကိုပဲဖတ်တာကိုး။နောက်ဆုံး LER ရောက်တဲ့အချိန်ကျတော့ Label Pop

လုပ်ပြီးပုံမှန် IP Packet အနေနဲ့ Destination ကို Forward လုပ်ပါတယ်။ ဒီပုံစံနဲ့ Label Switching အလုပ်လုပ်ပါတယ်။ MPLS ကိုတော့ Underlying IGP တစ်ခု Run ပြီးတော့ VRF, MP-BGP စတာတွေကိုအသုံးပြုပြီး MPLS Layer 3 VPN, MPLS Layer 2 VPN စသဖြင့် Service Provider တွေရဲ့ လက်သုံးတော်အနေနဲ့ သုံးကြပါတယ်။ Scalability အရမ်းကောင်းပြီး လွယ်ကူရိုးရှင်းပါတယ်။



MPLS VPN တွေအကြောင်းတစ္ဆေတစောင်း

MPLS L3VPN ဆိုတာက PE-Based SP VPN Solution တစ်ခုပါ။ BGP ကို သုံးပြီးတော့ VPN Route တွေကို Advertise လုပ်တယ်။ MPLS ကိုသုံးပြီးတော့ VPN Traffic ကို Forward လုပ်တယ်။ MPLS L3VPN Architecture မှာ Device (3) မျိုးပါဝင်ပါတယ်။

(1) CE

(2) PE

(3) P

CE = Customer Edge Router

→ CE ဆိုတာကတော့ Router (သို့မဟုတ်) Switch လည်းဖြစ်နိုင်သလို သာမန် End Device တစ်ခုလည်းဖြစ်နိုင်ပါတယ်။ သူမှာက VPN နဲ့ပတ်သက်ပြီး ဘာမှသိစရာမလိုသလို ၊ MPLS ကို Support မလုပ်လဲ ပြဿနာ မရှိပါဘူး။ Customer Network ရဲ့ Edge Device တစ်ခုပါပဲ။

PE = Provider Edge Router

→ PE ဆိုတာကတော့ Service Provider Network ရဲ့ Edge Device တစ်ခုပါပဲ။ CE များစွာနဲ့လက်ခံချိတ်ဆက်ရတဲ့ သူပေါ့။ MPLS Network မှာကတော့ VPN Processing အားလုံးကို သူ့မှာပဲ လုပ်ကြပါတယ်။

P = Provider Router

→ P ကတော့ Service Provider Network ရဲ့ Core Device ပါ။ ဘယ် CE နဲ့ မချိတ်ရပါဘူး။ (ကိုယ့်လိုအပ်ချက်အရ ချိတ်ချင်ချိတ်မှာပေါ့) ။ VRF, VPN Processing တွေကိုလည်း Handle လုပ်စရာမလိုပါဘူး။ (လိုရင် P ကလည်း ထုတ်သုံးမှာပေါ့ ၊ မလိုရင် မသုံးပါနဲ့) ။ သူ့မှာက IGP နဲ့ MPLS Basic Forwarding Capability ရှိရင်ရပါပြီ။

MPLS Architecture မှာ CE တွေနဲ့ PE တွေက SP နဲ့ Customer ရဲ့ Boundary ကိုခွဲခြားသတ်မှတ်ပေးပါတယ်။

CE အနေနဲ့ သူ့ရဲ့ Route တွေကို PE ကိုပို့မယ်။ PE အနေနဲ့က CE က လာတဲ့ Route တွေကိုလက်ခံမယ်။ ဘယ် CE က ပို့တာလဲ ဆိုတာခွဲခြားသိဖို့ VRF တွေခွဲပြီးလက်ခံမယ်။ ပြီးရင် သူနဲ့ဆိုင်ရာဆိုင်ရာ Remote PE ဆီကို VRF အလိုက် VPN Information အနေနဲ့ MPLS Backbone ကိုဖြတ်ပြီးပို့မယ်။ PE နဲ့ CE ကြားကတော့ BGP, IGP, Static ဒါတွေသုံးပြီး ချိတ်ဆက်လို့ရပါတယ်။

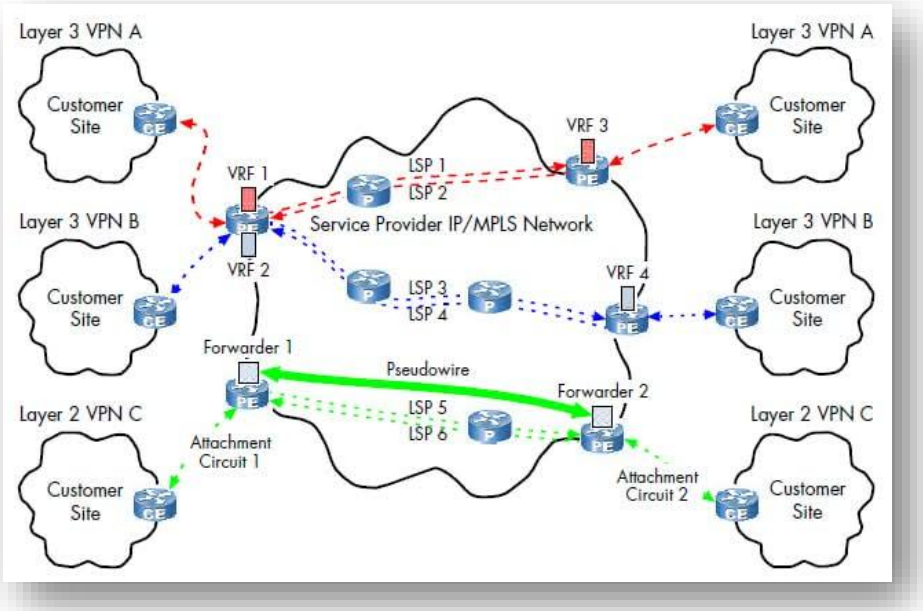
PE အနေနဲ့ကတော့ သူရရှိထားတဲ့ VPN Information တွေကို BGP ကိုသုံးပြီး ဆိုင်ရာဆိုင်ရာ PE အချင်းချင်း Exchange လုပ်ပါမယ်။ ပြောရရင် VPN Processing တွေကို သူ တာဝန်ယူရတယ်ပေါ့။ PE to PE ကို MPLS Backbone ထဲကနေ Tunnel အနေနဲ့သွားပါတယ်။

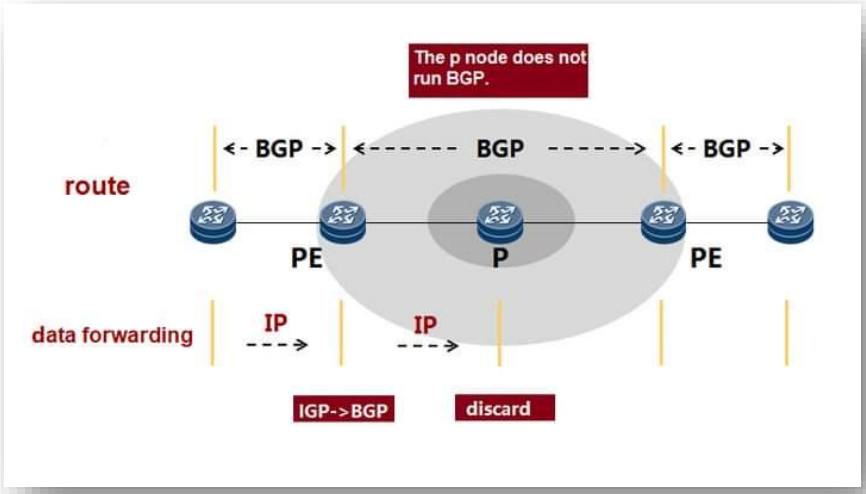
P အနေနဲ့ကတော့ အရမ်းရိုးရှင်းပါတယ်။ သူက PE တွေနဲ့ ချိတ်ဆက်ပြီးတော့ Backbone Switching လုပ်ပေးမယ် ၊Transport လုပ်ပေးမယ်ဒါပါပဲ။ VPN Processing နဲ့ VPN Information (VRF ဘာညာ စမာကလာ) တွေက သူနဲ့ဆက် နွယ်စရာ အကြောင်းမရှိပါဘူး။ Underlying Protocol တစ်ခုနဲ့ MPLS Enable လုပ်ထားရင်ကိုရပါပြီ။ ဒါမဲ့ ကိုယ့်ရဲ့ လိုအပ်ချက်အရ P ကနေမှ VPN ထုတ်သုံးချင်တယ်ဆိုရင်လဲ BGP Run ပြီးထုတ်သုံးရုံပါပဲ။ ဒါက အခြေခံပါ။ P Device တွေရဲ့ Management ကို VRF တစ်ခုအနေနဲ့ ယူချင်တဲ့အခါမျိုးမှာလဲ P Device တွေမှာ BGP Run ရပါတယ်။ နောက်တစ်ချက်က ကိုယ့်ရဲ့ SP Network က အရမ်းကြီးလို့ RR လိုမျိုး ထားရမယ်ဆိုရင်လည်း Core Device တွေထဲက Load နည်းပြီး Performance မြင့်တဲ့ Device မျိုးရွေးပြီး PE တွေက RR ကို Reflector ဝိုင်းထိုးကြပေါ့။ သဘောတရားအရကတော့ P တွေက BGP Run စရာမလိုပါဘူး။

ပြောရရင်တော့ MPLS Architecture မှာ CE, PE, P ပေါ့။ Control Plane Requirement ကတော့ Underlying IGP, MPLS. MP-BGP, VRF-Lite နဲ့ PE - CE Routing ပါပဲ။

MPLS Layer 2 VPN တွေဆိုတာကတော့ Layer 2 Network တွေကို Extend လုပ်ဖို့အတွက် MPLS Backbone ပေါ်မှာအသုံးပြုတဲ့ Technology တစ်ခုဖြစ်ပါတယ်။ ဒီ Technology ကို Service Provider တွေအနေနဲ့ အဓိကအသုံးပြုပါတယ်။

MPLS Layer 2 VPN (၂) မျိုးရှိပါတယ်။ Virtual Private Wire Services (VPWS) နဲ့ Virtual Private LAN Services (VPLS) တို့ဖြစ်ပါတယ်။ VPWS က Point-To-Point ဖြစ်ပြီးတော့ VPLS က Point-To-Multipoint ဖြစ်ပါတယ်။ နောက်တစ်ခုဖြစ်တဲ့ Hierarchical VPLS (H-VPLS) ကတော့ VPLS ရဲ့ Extension ဖြစ်ပါတယ်။





BGP Free Core

ဒီနေရာမှာ BGP Free Core အကြောင်းအနည်းငယ် ရှင်းပြလိုပါတယ်။ BGP Free Core ဆိုတာက.... Core မှာ BGP Free ဖြစ်နေတာပါ....LOL….။ Service Provider Network တွေမှာ MPLS လိုမျိုး အစရှိတဲ့ Tunnelling Mechanism တွေအသုံးပြုတဲ့အခါမှာ Core Device (P Device) တွေမှာ BGP run ဖို့မလိုတဲ့ Network Deployment ကို BGP Free Core လို့ခေါ်ပါတယ်။ Core Device တွေမှာ BGP မရှိတဲ့အတွက်ကြောင့် BGP Route တွေလက်ခံထိန်းသိမ်းထားစရာမလိုသလို BGP Related Issues တွေဖြစ်တဲ့ CPU Utilization တက်တာတွေ မဖြစ်တော့ဘူးပေါ့။ MPLS VPN တွေ EVPN တွေ Implement လုပ်ခဲ့ရင်လည်း Core Device တွေကိုထိစရာမလိုတဲ့အတွက်ကြောင့် သက်သာတာပေါ့။

MPLS Security

MPLS L2/L3 VPN တွေကလုံခြုံမှုစိတ်ချရလား …..

MPLS VPN Model ဆိုတာကတော့ Scale အရမ်းကောင်းတဲ့ Model တစ်ခုပါပဲ။ Customer တွေအနေနဲ့ Site To Site တွေ လုံလုံခြုံခြုံ Connect လုပ်နိုင်တဲ့ Model တစ်ခုပါပဲ။ ဒီနေရာမှာတစ်ခုစဉ်းစားစရာက MPLS Circuit တွေနဲ့ပတ်သက်လို့ ဘာ Encryption တွေပါသလဲပေါ့။ ပုံမှန်အားဖြင့်တော့ MPLS VPN က ဘာ Encryption မှ မပါပါဘူး။ ဒါပေမဲ့ အကယ်၍ ကျွန်တော်တို့ Network တွေ၊ Device တွေမှာ Major Bug တွေ ၊ Configuration ပိုင်းဆိုင်ရာ အမှားအယွင်းတွေသာမရှိဘူးဆိုရင် MPLS Circuit တွေ ၊ Internal Networks တွေကို Expose ဖြစ်ဖို့ မလွယ်ကူပါဘူး။ ဒါကိုမှ လုံခြုံမှုရချင်တယ်ဆိုရင်တော့ ထုံးစံအတိုင်းကျွန်တော်တို့ရဲ့ လုံခြုံရေးဇာတ်လိုက်ကြီး IPSec ကိုခေါ်သုံးရုံပေါ့။ End Points တွေကြားက IP Based Pathway တွေအတွက် အကောင်းဆုံး Protocol Suite ကြီးလေ။ ဘယ်လိုသုံးမလဲဆိုရင်တော့....

(1) CE - CE IPSec

(2) PE - PE IPSec

[CE - CE IPSec]

CE အချင်းချင်း IPSec Tunnel ဖောက်လိုက်ခြင်းအားဖြင့် CE တွေကြားက Path တစ်ခုလုံးက Protect ဖြစ်ပြီးသားပေါ့။ CE ကို Packet တွေစဝင်လာပြီဆိုကတည်းက Encrypted ဖြစ်ပြီးသားပဲပေါ့။ Peer CE ဖက်ရောက်တာနဲ့ Decrypted လုပ်ပြီး ထွက်သွားရုံပဲ။ ဒါပဲပေါ့။ ဘာတွေကာကွယ်ပေးသလဲ ကြည့်မယ်။

(1) Anti-Replay

(2) Man-in-the-Middle

(3) P, PE, CE တွေမှာ Eavesdropping လုပ်တာတို့ပေါ့။

[PE - PE IPSec]

ဒီ Method ကတော့ CE - CE IPSec လောက်တော့ Secure မဖြစ်ဘူးပေါ့။ ဘာလို့လဲဆို PE ရောက်မှ Encrypted စဖြစ်တာကိုး။ ပြောရရင် VPN တစ်ခုရဲ့ Security Scheme နဲ့မညီဘူးပေါ့လေ။ သူကတော့....PE တွေ P တွေမှာ Eavesdropping (အလွယ်ပြောရရင် ခိုးနားထောင်တာ) လုပ်မရဘူးပေါ့။ Point-to-Point Link တွေမှာ လွယ်ပေမဲ့လဲ Multi-Point တွေဆိုရင်တော့ ခက်ခဲရှုပ်ထွေးတာပေါ့။ IPSec ရဲ့ သဘောတရားတွေအရ Configuration ရှုပ်ထွေးမှုရှိတာကိုး။ ဒါကတော့ အားလုံးသိပြီးသား ဖြစ်ကြမှာပါ။

သာမန်အားဖြင့် MPLS VPN တွေကို ဘယ်လိုကာကွယ်ကြမလဲ ဆိုရင် တော့ MPLS Router တွေကို Attack တွေရန်က ကာကွယ်ဖို့အတွက် Network မှာ အားလုံးသိကြပြီး Techniques တွေဖြစ်တဲ့ Packet Filtering လုပ်တာတွေ၊ ACL သုံးတာတွေ ၊ Protocol တွေမှာ မလိုအပ်တဲ့ Port တွေ ရွေးပိတ်ထားတာမျိုးတွေ၊ Neighbor Authentication ခံထားတာမျိုးတွေကိုသုံးလို့ရပါတယ်။ ကိုယ့် Network မှာ သုံးထားတဲ့ Protocol တွေမှာပါတဲ့ Built-in Security Features တွေကို Enabled လုပ်ထားတာမျိုး၊ Level Up လုပ်ထားတာမျိုးတွေလဲ လုပ်လို့ရပါတယ်။ ဥပမာပြောရရင်.... BGP, OSPF တွေမှာ Authentication (MD5, SHA) သုံးထားတာမျိုးတွေ၊ VRF တွေမှာ Maximum Route အရေအတွက် သတ်မှတ်ပေးထားတာမျိုးတွေပေါ့။ ဒီလောက်ဆိုရင်တော့ MPLS အကြောင်း အကြမ်းဖျဉ်း နားလည်သဘောပေါက်လောက်ပြီထင်ပါတယ်။

ကိုလွင် (Network)