

## **Autenticação através de MPLS/VPLS**

**Eduardo Braum**

**Fernando Klabunde**



**wavetec**  
Fones: (54) 3329-1708 / 3331-8509 / 9905-0024

*Fibra Óptica de alta performance*

**PLANOS Fibra Óptica**  
Para você que necessita de internet de alta performance!  
  
[SAIBA MAIS](#)

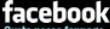
**PLANOS Via Rádio**  
Internet de alta velocidade pelo melhor custo x benefício!  
  
[SAIBA MAIS](#)

**Entre em Contato**  
Para realizar contato conosco preencha todos os campos. Retornaremos o mais breve possível a sua mensagem.

nome  
email  
telefone  
cidade  
estado  
mensagem  
[ENVIAR](#)

**Conheça a Wavetec**  
  
A Wavetec Comunicações é uma empresa carazinhense com mais de 12 anos de experiência na área de Provedor de Serviços de Internet (ISP), além de comercialização de equipamentos de comunicação de dados, tendo à disposição profissionais qualificados para prover e gerenciar ambientes Profissionais e Corporativos de alta complexidade.  
[SAIBA MAIS](#)

 Empresa autorizada  
**ANATEL**  
53528.000947/2002

 facebook  
Curta nossa fanpage

Wavetec Comunicações  
Av. Flores da Cunha, 1455  
Sala 304 - Carazinho/RS

**agfox**  
agência web

## Índice da apresentação

- \* A estrutura da empresa
  - \* Problemas vividos
  - \* Soluções estudadas e adotadas
- 
- \* MPLS
  - \* VPLS
  - \* Estudos de caso
  - \* Implementação
  - \* Considerações finais

## A Empresa

- \* A mais de 13 anos na atividade de provedor de internet para Carazinho e região do planalto médio gaúcho;
- \* Pertencente ao **Grupo Razaoinfo** de Passo Fundo/RS;
- \* Empresa líder do segmento Internet dentro da região Norte do Rio Grande do Sul com foco em prestar um serviço de qualidade e com alta tecnologia;

## Estrutura

- \* Mais de 1Gb de link contratados com operadoras Telecom;
- \* Utilização de AS e BGP com operadoras;
- \* Fibra-óptica para a entrega principal de link;
- \* Redundância no recebimento de link através de rádios de frequência fechada;
- \* Hardwares mistos dentro do Data Center;
- \* Mais de 50 POP's para distribuição de sinal;
- \* Ampliando backbone Gpon para entrega de fibra óptica;
- \* Atualmente usando apenas FTTB e “FTTC”;

## Estrutura antiga de rede

- \* Toda a rede em bridge;
- \* Autenticação do cliente através de IP;
- \* Controle de MAC por access-list;
- \* Seguidas quedas de rede por looping e/ou “estouros” de broadcast;
- \* Performance baixa;
- \* Latência alta;

## As alternativas - Parte I

- \* Segmentar a rede;
- \* Roteamento nas células;
- \* Hostspot no escritório;
- \* PPPoE no escritório - *Solução adotada em paralelo com a estrutura antiga;*

## Resultado - Parte I

- \* De inicio funcionou bem;
- \* Um único servidor não atendia toda a demanda;
- \* Necessário direcionar os clientes para um segundo servidor;
- \* Rede estava crescendo muito rápido e problemas se agravando;

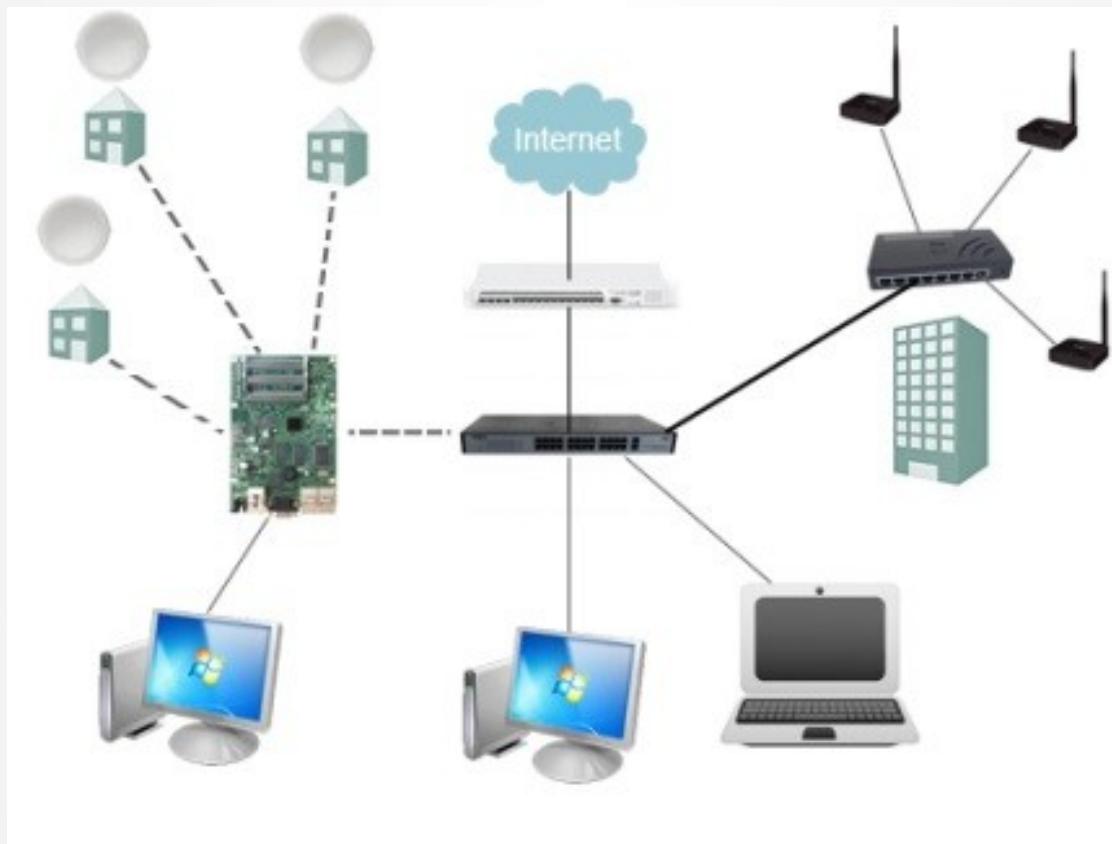
## As Alternativas - Parte II

- \* Concentrar clientes PPPoE na célula;
- \* VLAN das células até os servidores;
- \* Segmentação física da rede (Isolar as células por porta de rede em cada servidor);
- \* MPLS/VPLS (Criar uma “nuvem” MPLS e fazer o tunelamento da célula até cada servidor) sendo está a *adotada*;

## MPLS

- \* O MPLS (Multiprotocol Label Switching) é um protocolo de roteamento **baseado em pacotes rotulados**;
- \* O objetivo de uma rede MPLS não é o de se conectar diretamente a sistemas finais. Ao invés disto ela é uma **rede de trânsito, transportando pacotes entre pontos de entrada e saída**;
- \* Padrão que foi feito com base em diversas tecnologias similares desenvolvidas por diferentes fabricantes. Ele é referido por documentos do IETF como sendo uma **camada intermediária entre as camadas 2 e 3**, fazendo com que estas se “encaixem” melhor;

## Rede Bridge

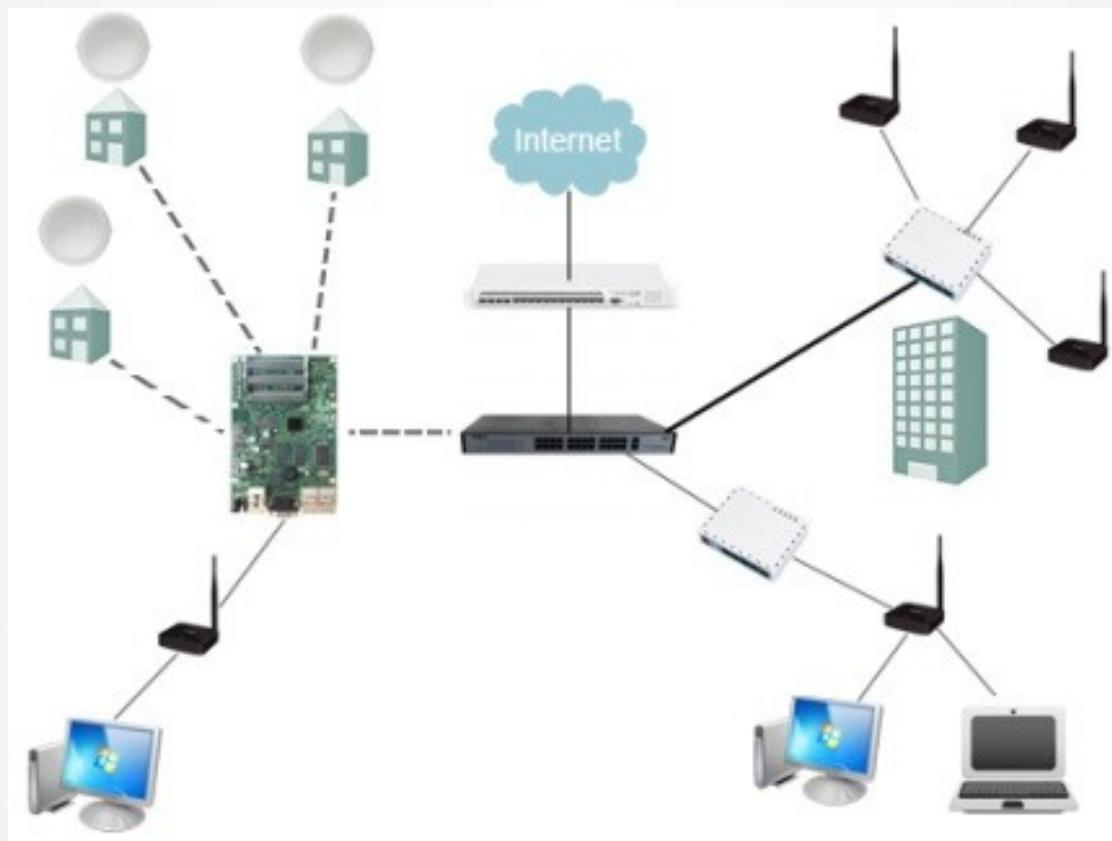


Autenticação através de MPLS/VPLS

## Rede Bridge

- \* Impossível montar a nuvem MPLS em uma rede sem equipamentos que suportem o protocolo MPLS;
- \* Rede vulnerável até mesmo a problemas com vírus nas máquinas ligadas diretamente na rede;
- \* Clientes finais não devem ficar ligados diretamente no core da rede, evitar de todas as maneiras deixar que qualquer dispositivo que não tenha como finalidade o transporte aos clientes estarem no core;

## Rede Ideal



Autenticação através de MPLS/VPLS

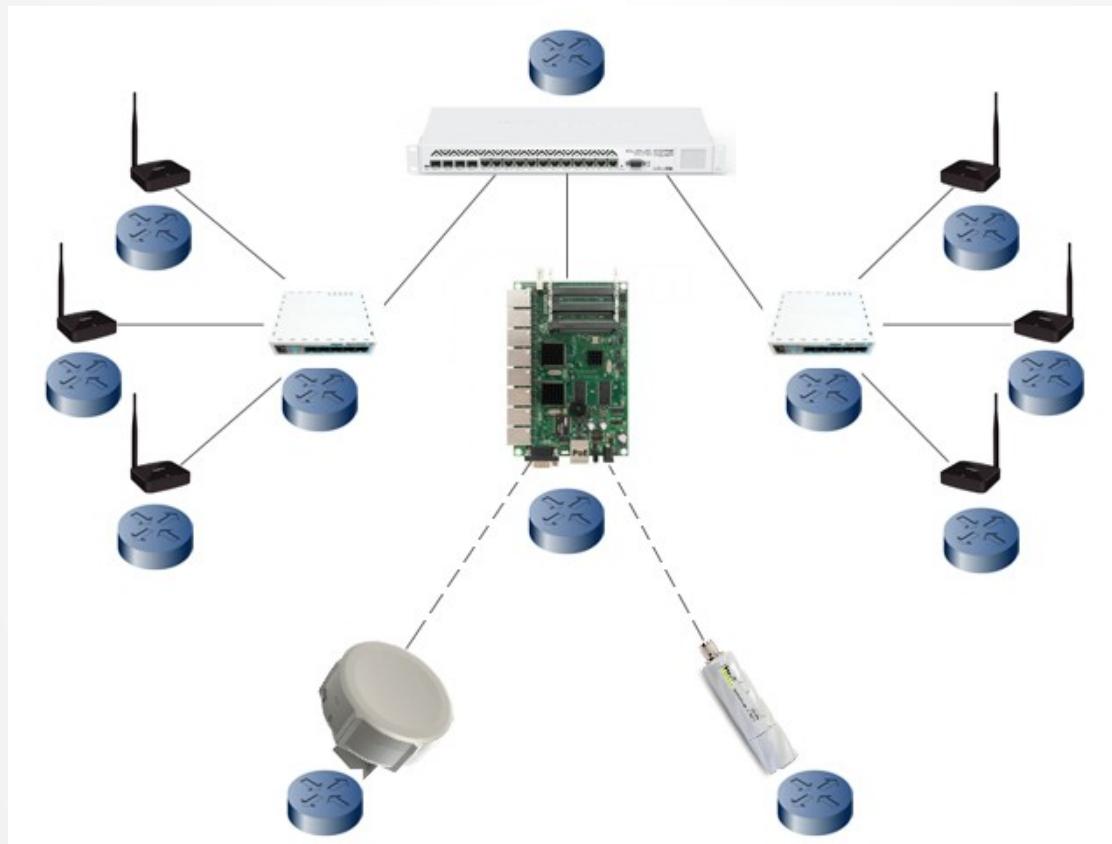
## Rede Ideal

- \* Independente da forma como o link chega até o nó de rede que atende o cliente, será necessário um equipamento que suporte o protocolo MPLS;
- \* Cliente final com computador isolado por roteamento ou NAT seja na antena(casa) ou no roteador(prédio);
- \* Somente equipamentos da empresa no core de rede, impedindo qualquer tipo de looping típico em redes Bridge causados até mesmo por um cabo com as 2 pontas ligados no mesmo Hub.

## VPLS

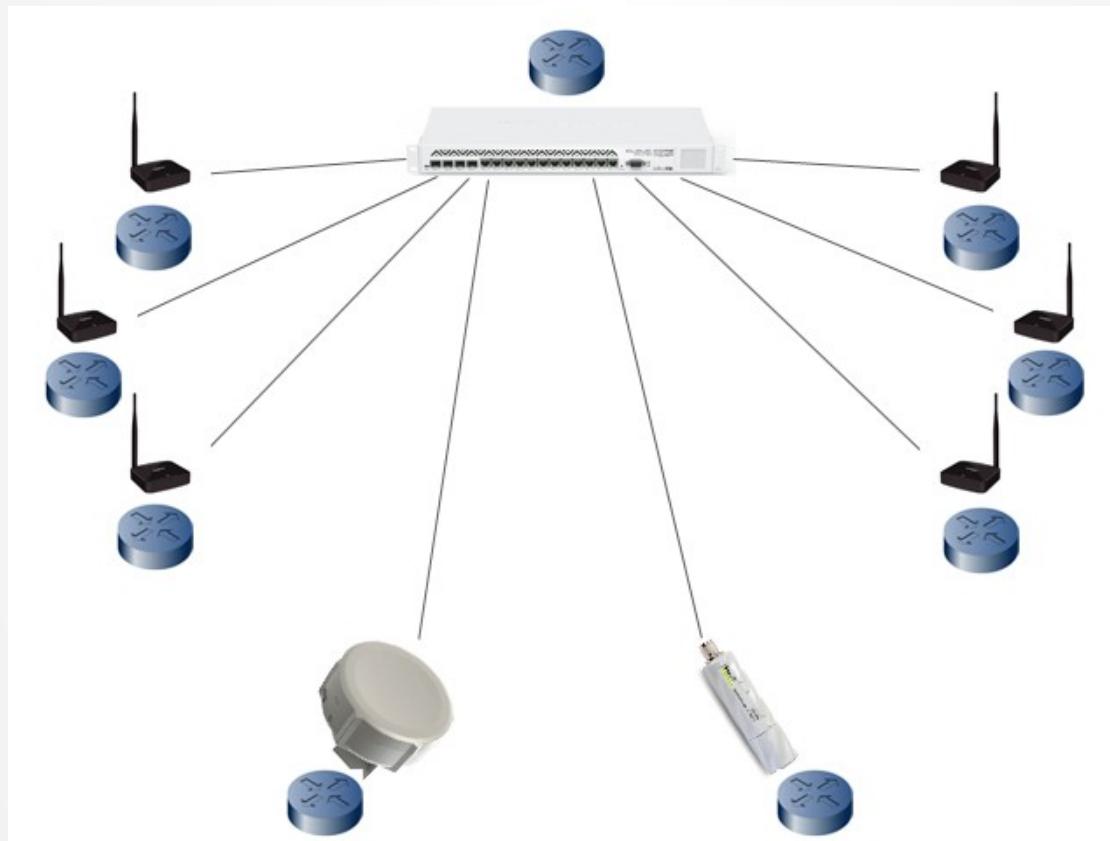
- \* VPLS, ou Virtual Private LAN Service, é usado para “emular” uma rede local sobre uma rede MPLS;
- \* Na visão do cliente toda a rede do provedor é vista como um grande “Hub”;
- \* Toda comunicação entre os pontos interligados é feita a nível 2 da camada OSI. O provedor de serviços analisará o pacote apenas até a camada de enlace, ignorando completamente as informações no cabeçalho da camada de rede.

## VPLS – Visão do provedor



# Autenticação através de MPLS/VPLS

## VPLS – Visão do cliente



Autenticação através de MPLS/VPLS

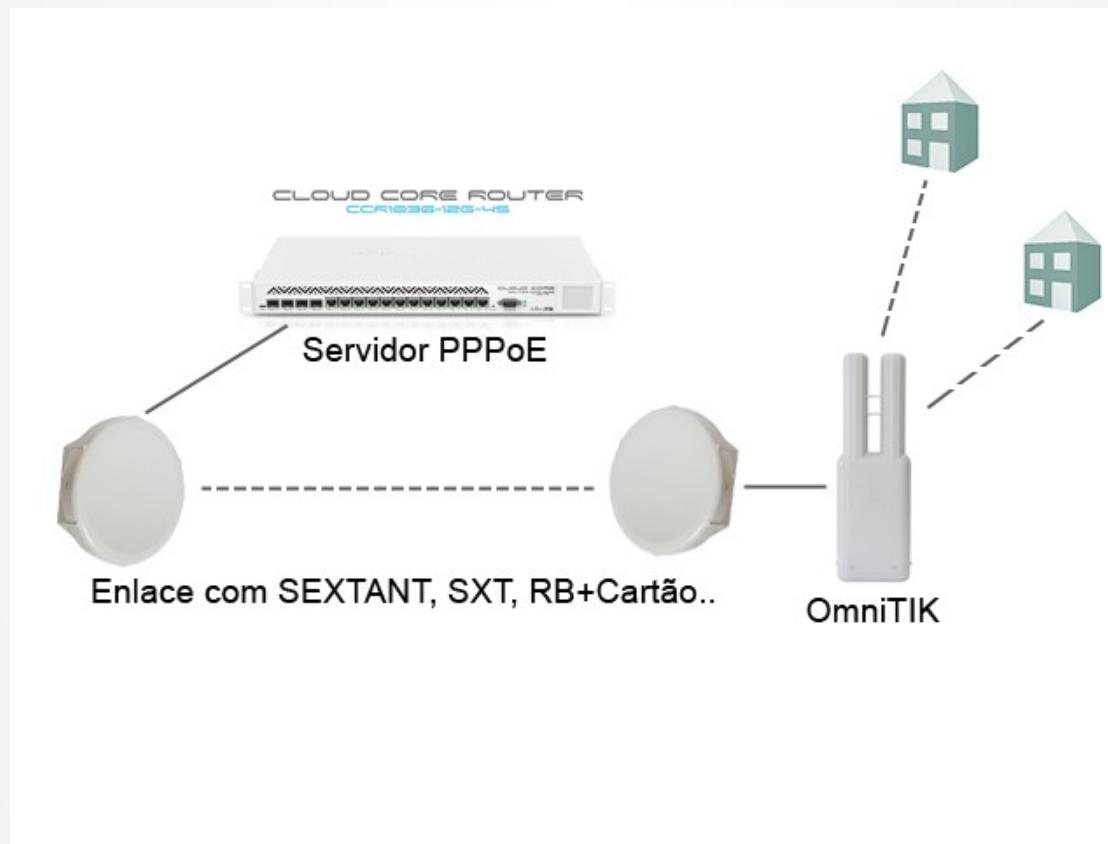
## Vantagens e Desvantagens

- \* Carga de CPU mais baixa que uma rede puramente roteada, o roteador somente analisa o rótulo do pacote e encaminha ao túnel via MPLS.
- \* Fornece transparência a uma rede roteada, com segurança efetiva, e com possibilidade de contingencia;
- \* Requer alto conhecimento técnico;
- \* Requer análise de MTU de toda a rede para que seja possível estabelecer os túneis;

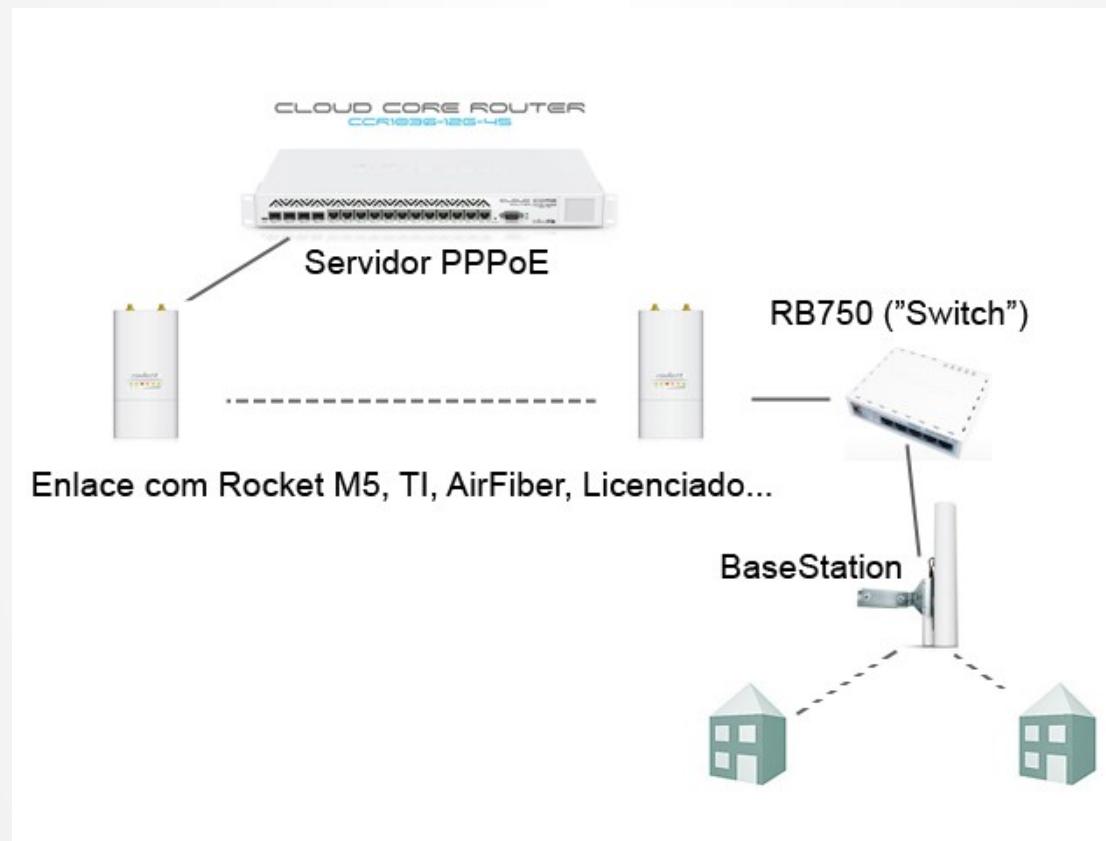
## Casos de estudo



## Casos de estudo

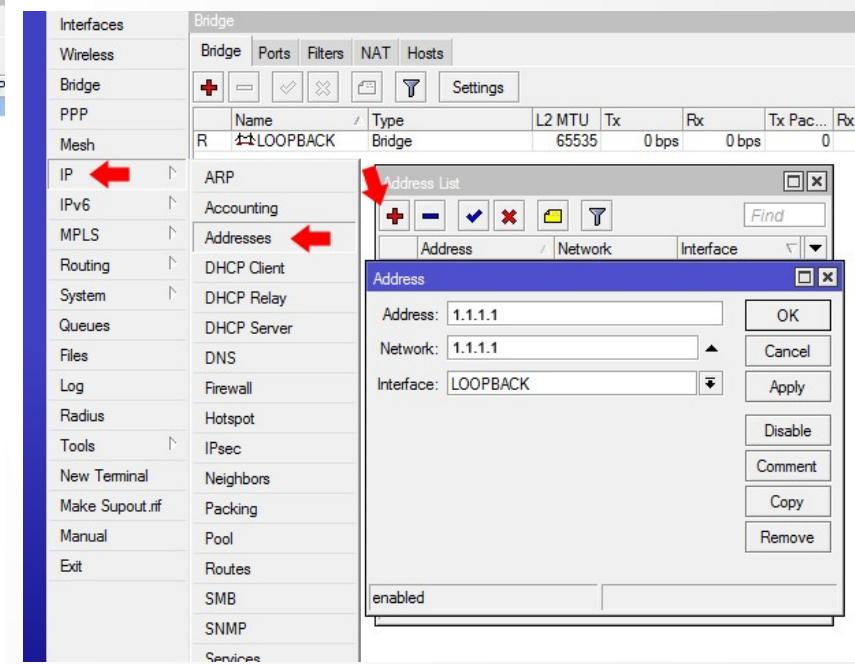
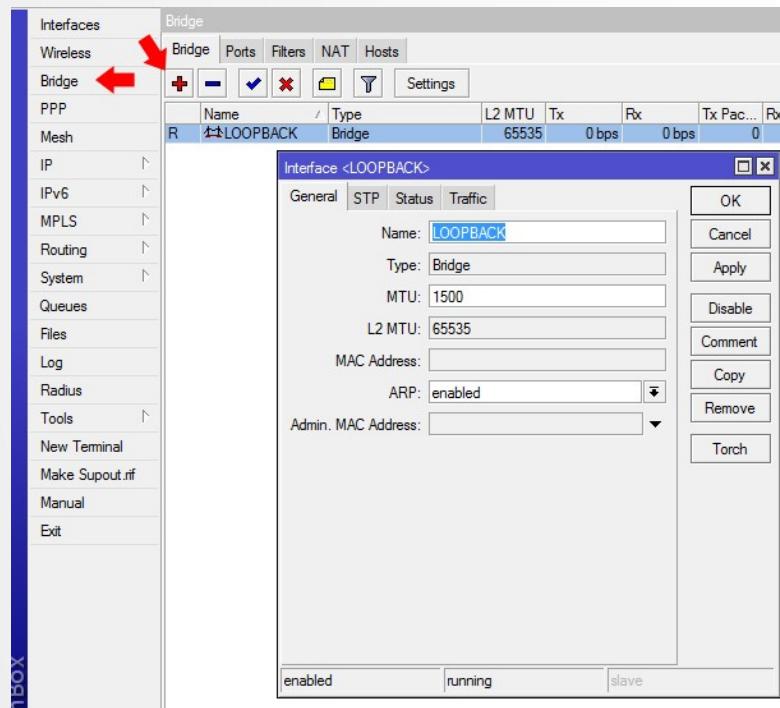


## Casos de estudo



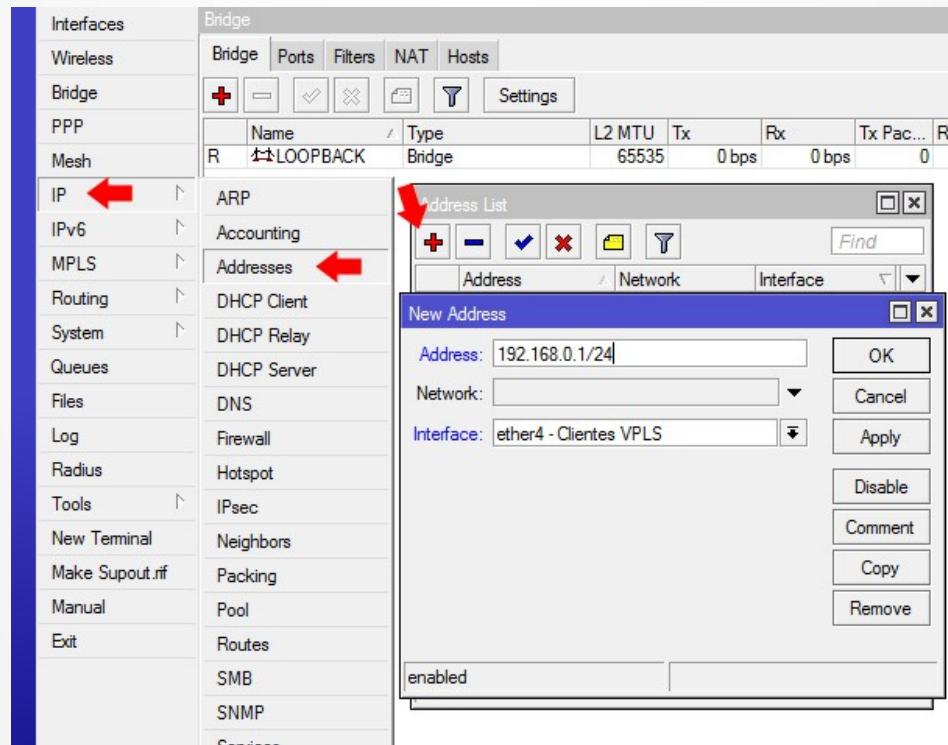
## Configuração – Servidor

- \* Adicionar interface LOOPBACK;
- \* Atrelar endereço /32 a LOOPBACK;



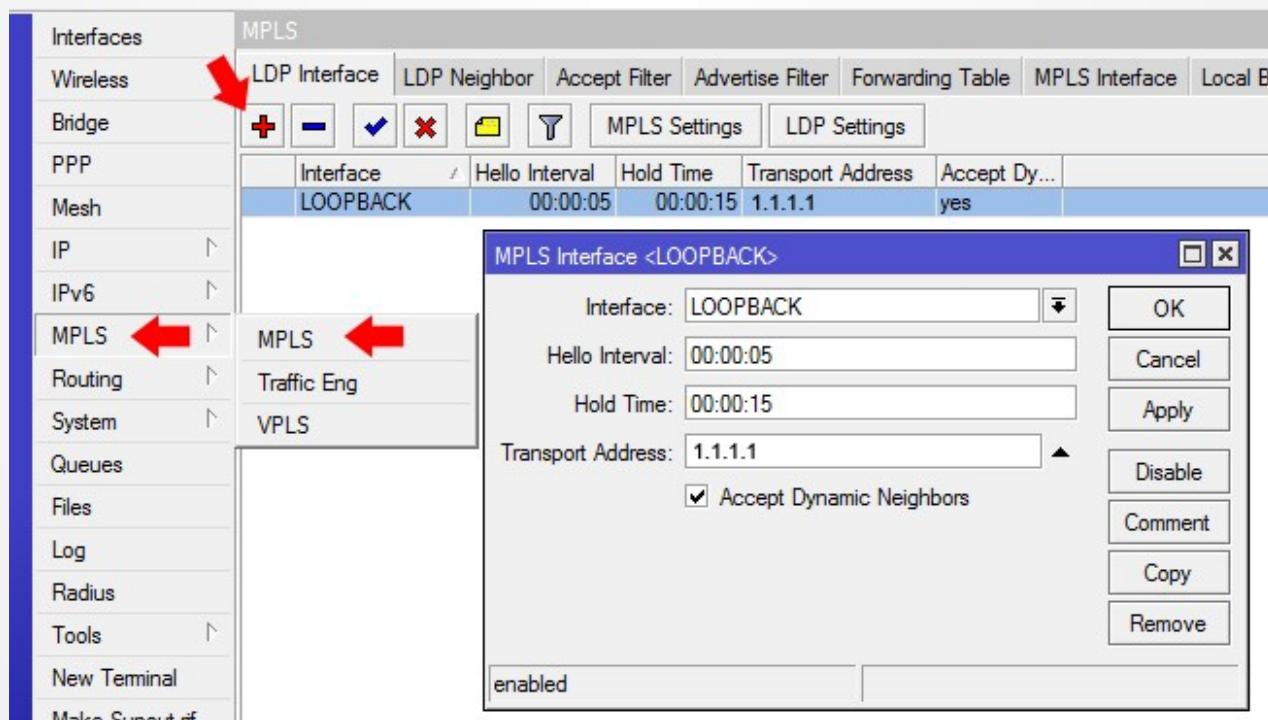
## Configuração – Servidor

\* Adicionar endereço a interface em bridge com o destino a ser configurado;



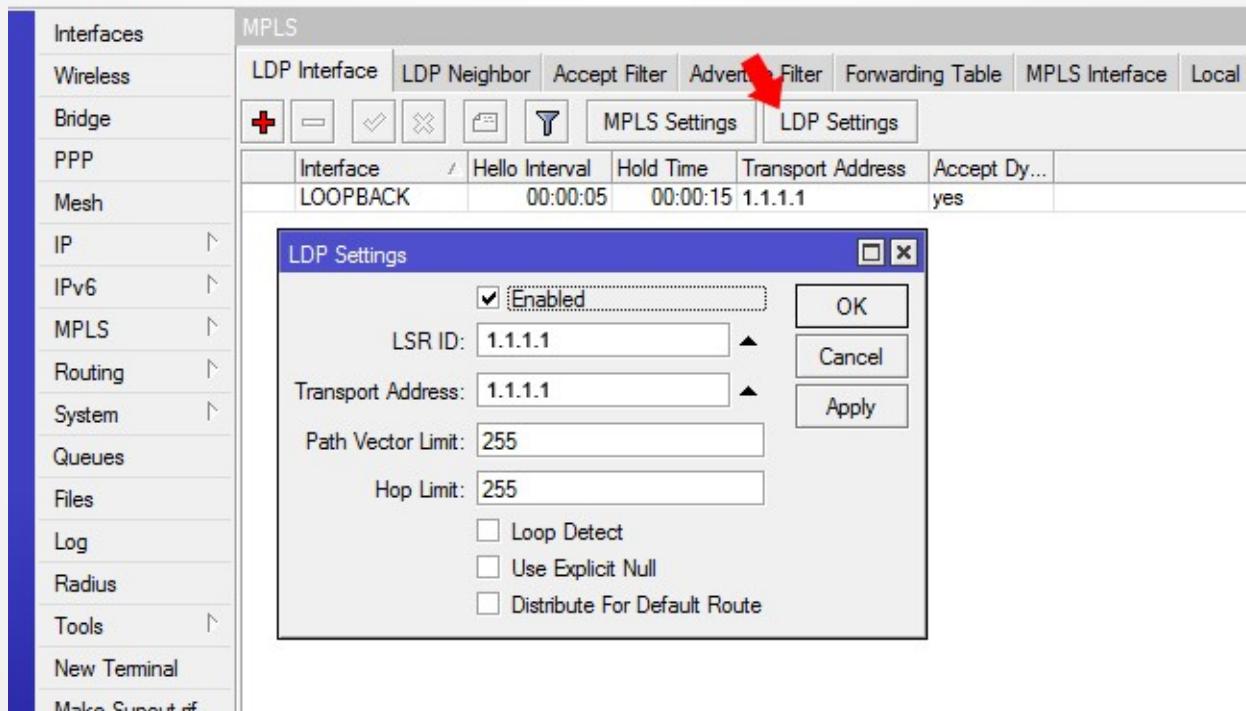
## Configuração – Servidor

- \* Menu: MPLS->MPLS;
- \* Adicionar a interface LOOPBACK em LDP Interface com seu endereço /32 da LOOPBACK;



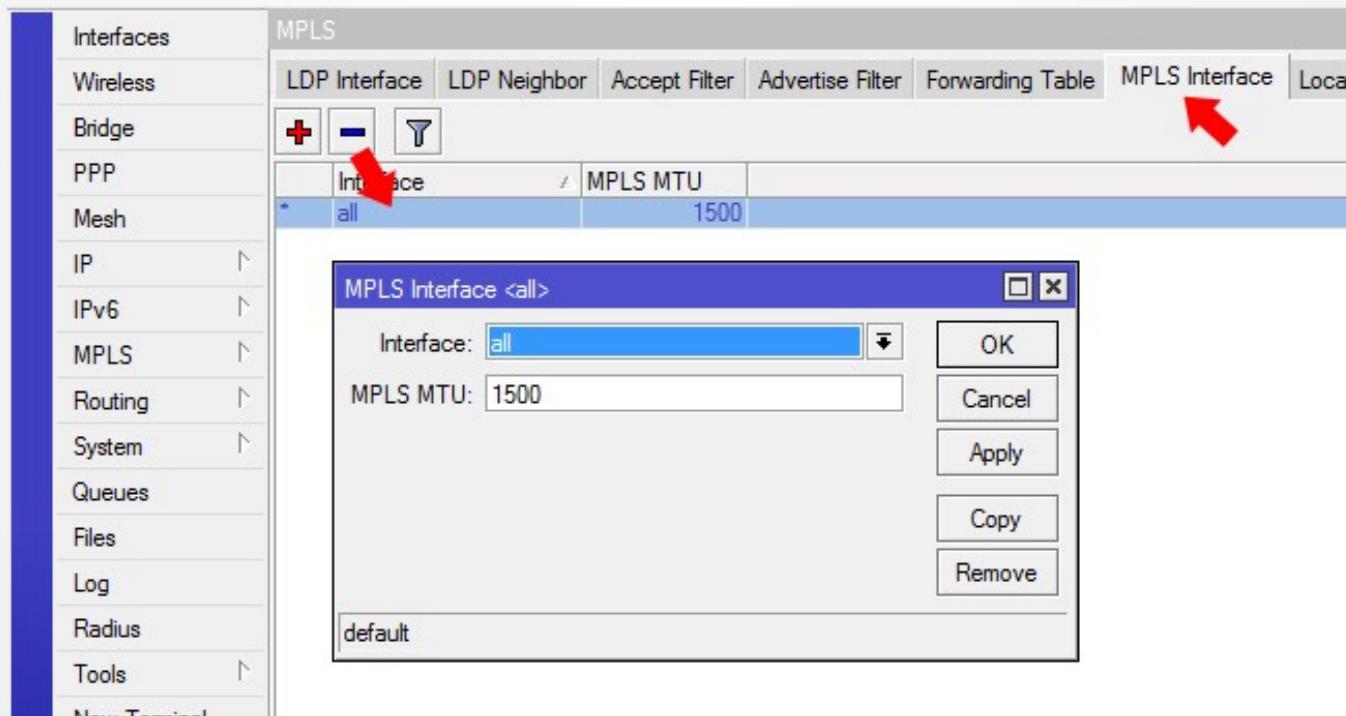
## Configuração – Servidor

- \* Menu: MPLS->MPLS;
- \* Acessar LDP Settings selecionar ENABLED;
- \* LSR ID e Transport Address deverá ser o endereço /32 da LOOPBACK;



## Configuração – Servidor

- \* Menu: MPLS->MPLS->MPLS Interface;
- \* Todos equipamentos da bridge estão adequados para suportar MTU maior que 1500?



## Configuração – Servidor

\* L2MTU

[http://wiki.mikrotik.com/wiki/Manual:Maximum\\_Transmission\\_Unit\\_on\\_RouterBoards](http://wiki.mikrotik.com/wiki/Manual:Maximum_Transmission_Unit_on_RouterBoards)

RouterBoard	MTU description
<b>RB Groove series</b>	ether1:2028
<b>RB Metal series</b>	ether1:2028
<b>RB SXT series</b>	ether1:2028
<b>RB SXT Lite series</b>	ether1:2028
<b>RB SXT G series</b>	ether1:4076
<b>RB750</b>	ether1:4076; ether2-ether5:2028
<b>RB750UP</b>	ether1:4076; ether2-ether5:2028
<b>RB751U-2HnD</b>	ether1:4076; ether2-ether5:2028
<b>RB OmniTik series</b>	ether1:4076; ether2-ether5:2028
<b>RB951-2n</b>	ether1:4076; ether2-ether5:2028
<b>RB951Ui-2HnD</b>	ether1:4076; ether2-ether5:2028
<b>RB750GL</b>	ether1-ether5:4074
<b>RB751G-2HnD</b>	ether1-ether5:4074
<b>RB951G-2HnD</b>	ether1-ether5:4074
<b>RB1200</b>	ether1-ether5:4078, ether6-ether8:4080, ether9-ether10:9116
<b>RB1100AH</b>	ether1-ether10:9498, ether11:, ether12-ether13:9116
<b>RB1100Hx2</b>	ether1-ether10:9498, ether11:9500, ether12-ether13:9116
<b>RB1100AHx2</b>	ether1-ether10:9498, ether11:9500, ether12-ether13:9116
<b>CCR series</b>	ether1-ether12:10226
<b>CRS125-24G-1S</b>	ether1-ether24:4064, sfp1:4064

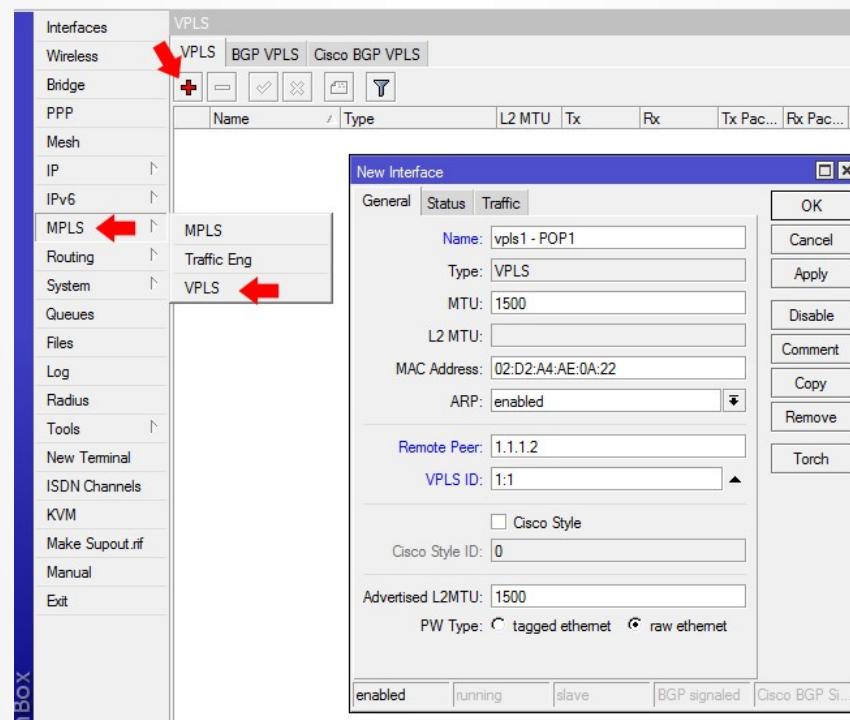
RouterBoard	MTU description
<b>RB411 series</b>	ether1:1526
<b>RB433 series</b>	ether1:1526; ether2-ether3:1522
<b>RB450</b>	ether1:1526; ether2-ether5:1522
<b>RB493 series</b>	ether1:1526; ether2-ether9:1522
<b>RB411GL</b>	ether1:1524
<b>RB433GL</b>	ether1-ether3:1524
<b>RB435G</b>	ether1-ether3:1520
<b>RB450G</b>	ether1-ether5:1520
<b>RB493G</b>	ether1-ether9:1520
<b>RB711 series</b>	ether1:2028
<b>RB711G series</b>	ether1:4076
<b>RB800</b>	ether1-ether2:9500; ether3:9116
<b>RB911G</b>	ether1:4076
<b>RB912UAG</b>	ether1:4076
<b>RB2011 series</b>	ether1-ether5:4074; ether6-ether10:2028; sfp1:4074
<b>RB44Ge</b>	ether1-ether4:9116

RouterBoard	MTU description
<b>RB600 series</b>	ether1-ether3:9500
<b>RB1000</b>	ether1-ether4:9500
<b>RB1100</b>	ether1-ether10:9498; ether11-ether13:9116
<b>RB750G</b>	ether1-ether5:1524

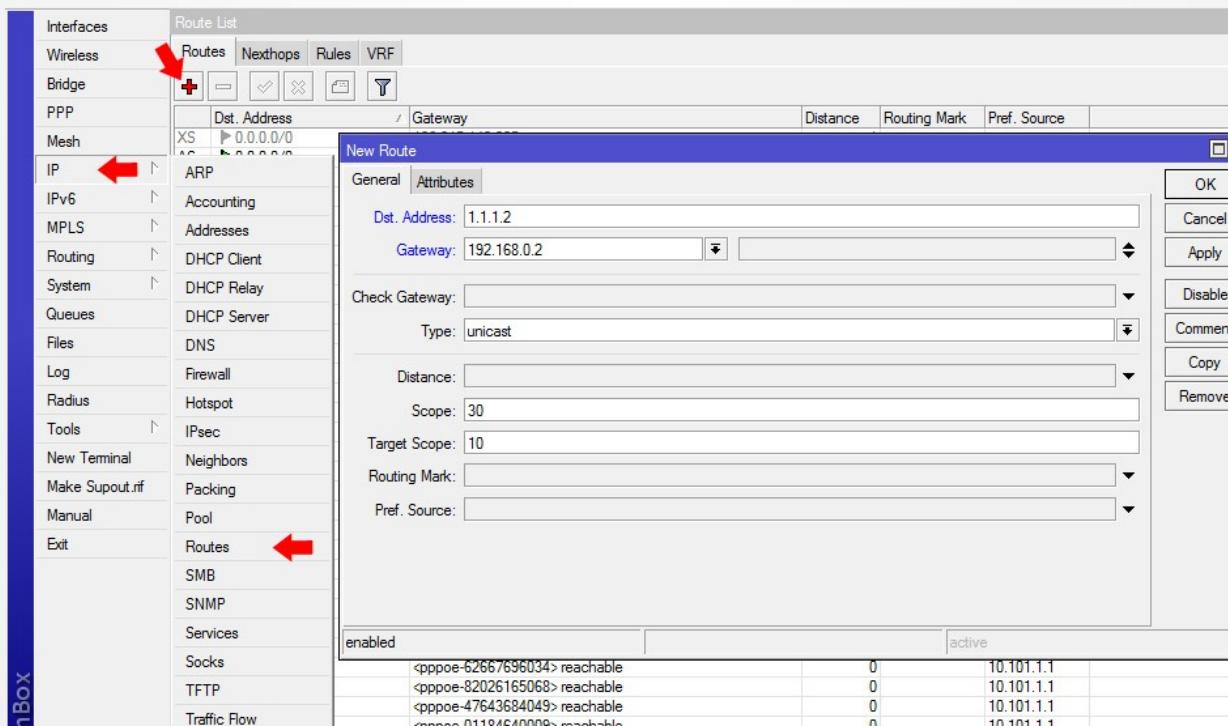
## Configuração – Servidor

- \* Menu: MPLS->VPLS;
- \* Adicionar uma nova VPLS com o IP da LOOPBACK do destino;
- \* Designar um ID (Rótulo) para esse túnel;



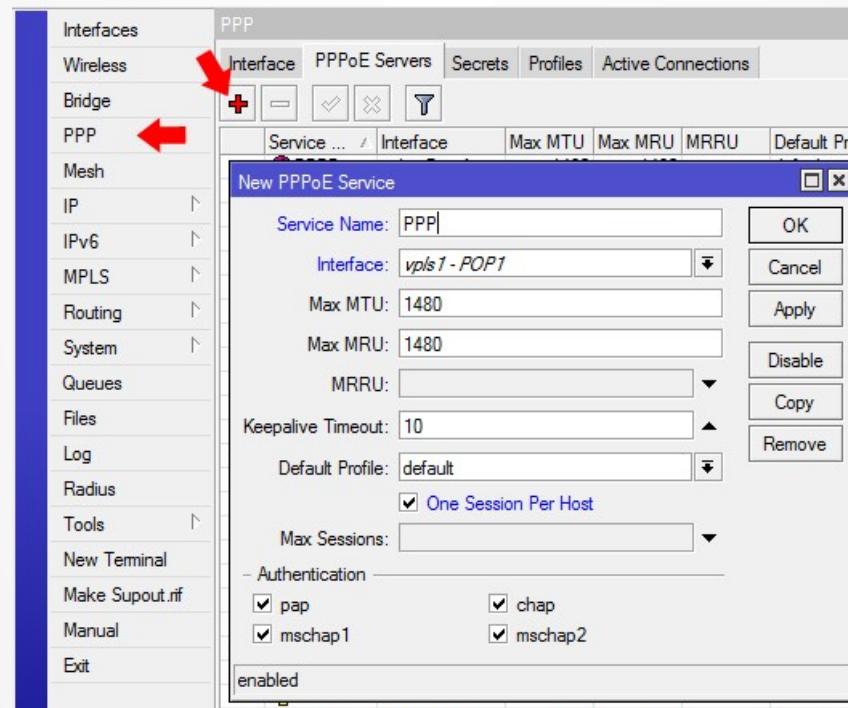
## Configuração – Servidor

- \* Menu: IP->Routes;
- \* Informar a rota de onde está a LOOPBACK do outro equipamento;
- \* Obs: Pode ser implementado OSPF;



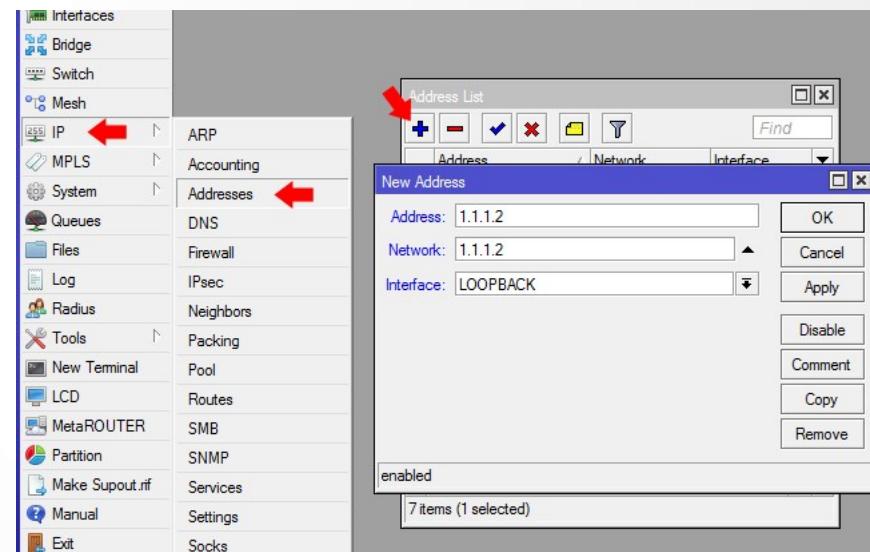
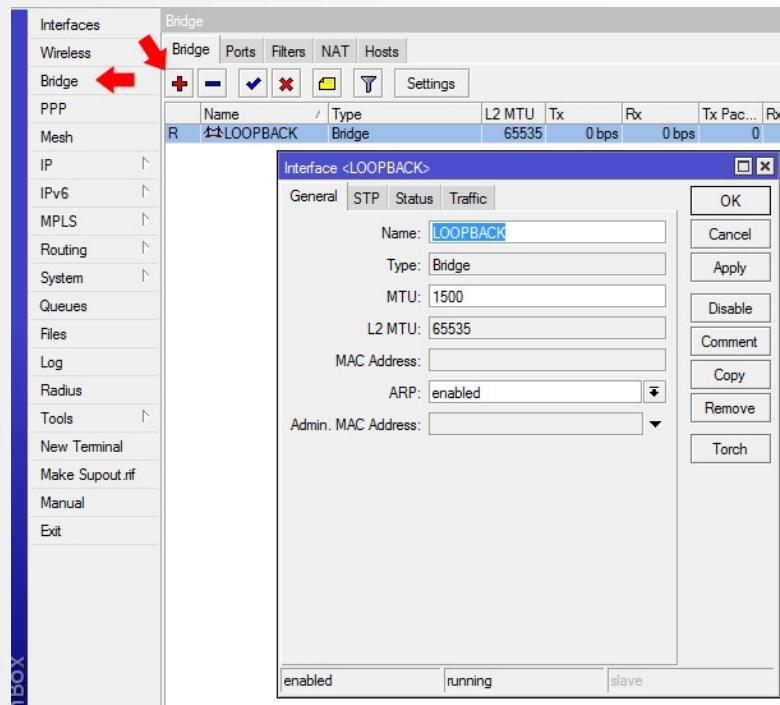
## Configuração – Servidor

- \* Menu: PPP->PPPoE Server;
- \* Adicionar um novo servidor PPPoE ao túnel VPLS criado;
- \* Poderia ser um Hotspot, ou até mesmo um IP na interface VPLS;



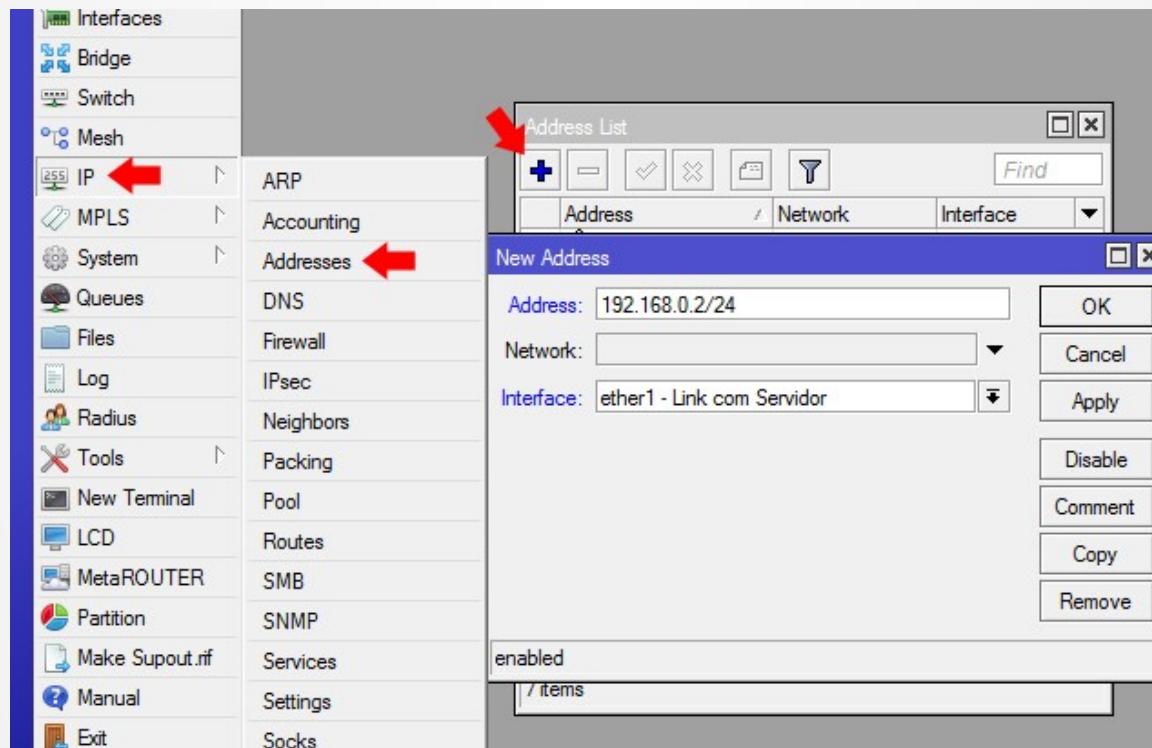
## Configuração – Destino

- \* Adicionar interface LOOPBACK;
- \* Atrelar endereço /32 a LOOPBACK;



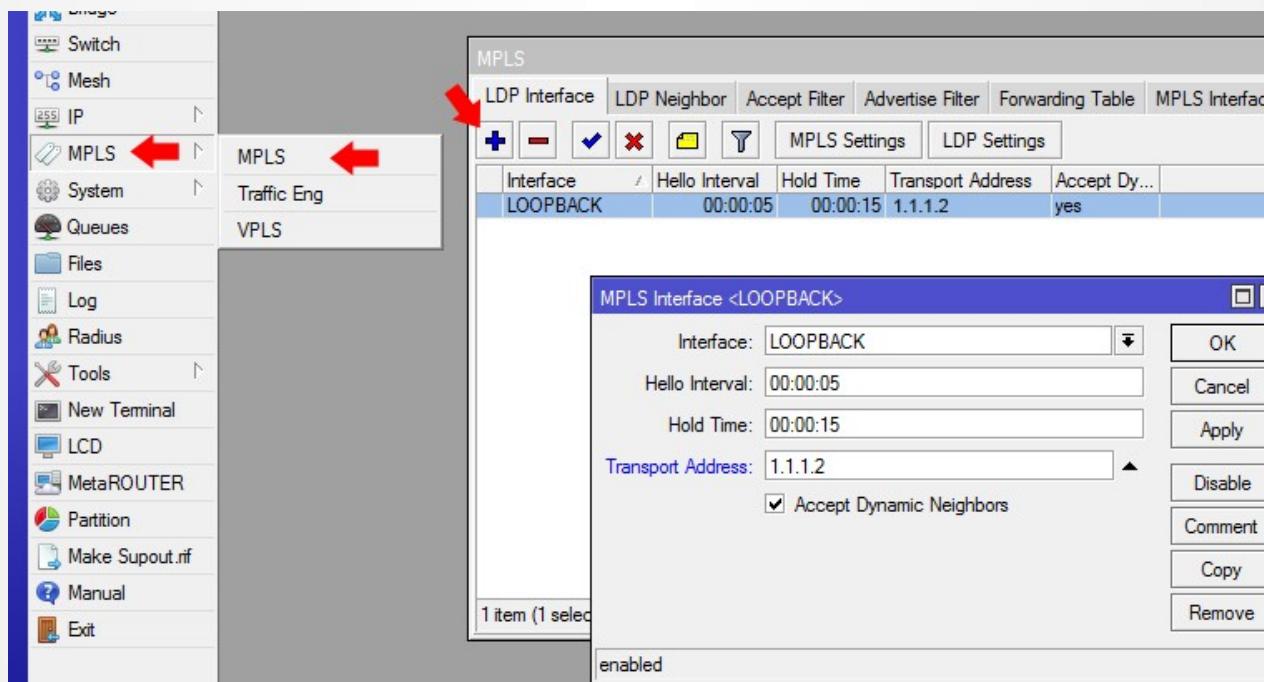
## Configuração – Destino

\* Adicionar endereço a interface em bridge com o servidor;



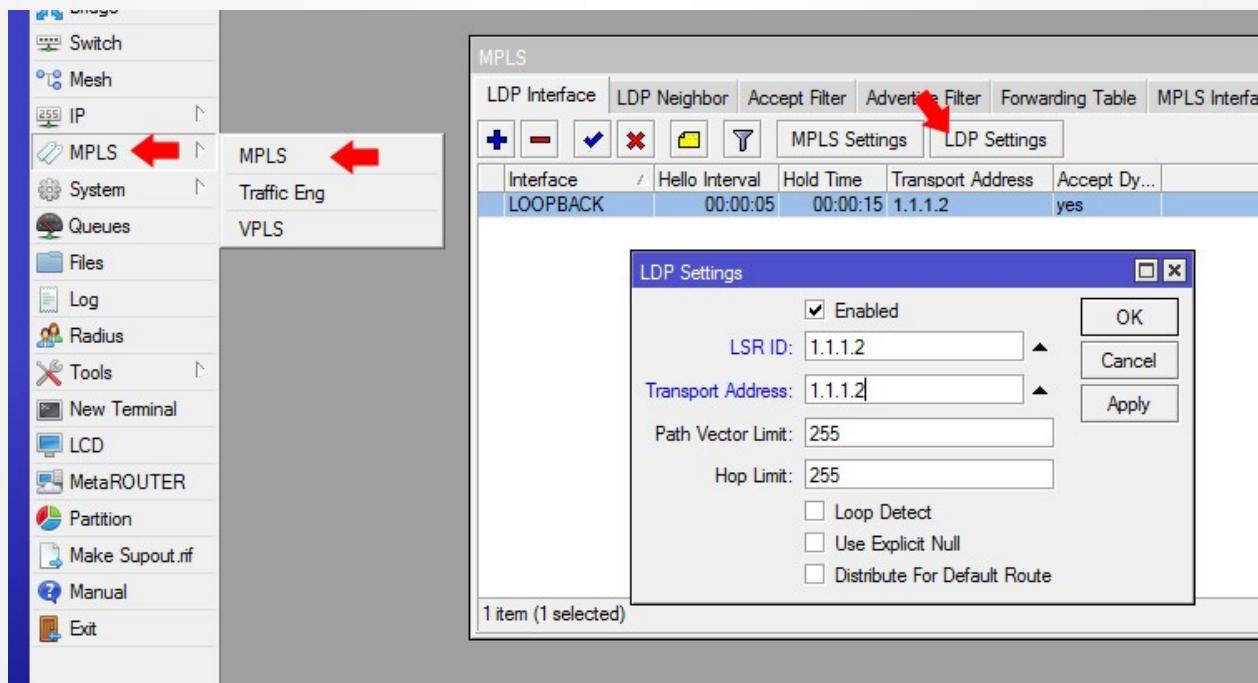
## Configuração – Destino

- \* Menu: MPLS->MPLS;
- \* Adicionar a interface LOOPBACK em LDP Interface com seu endereço / 32 da LOOPBACK;



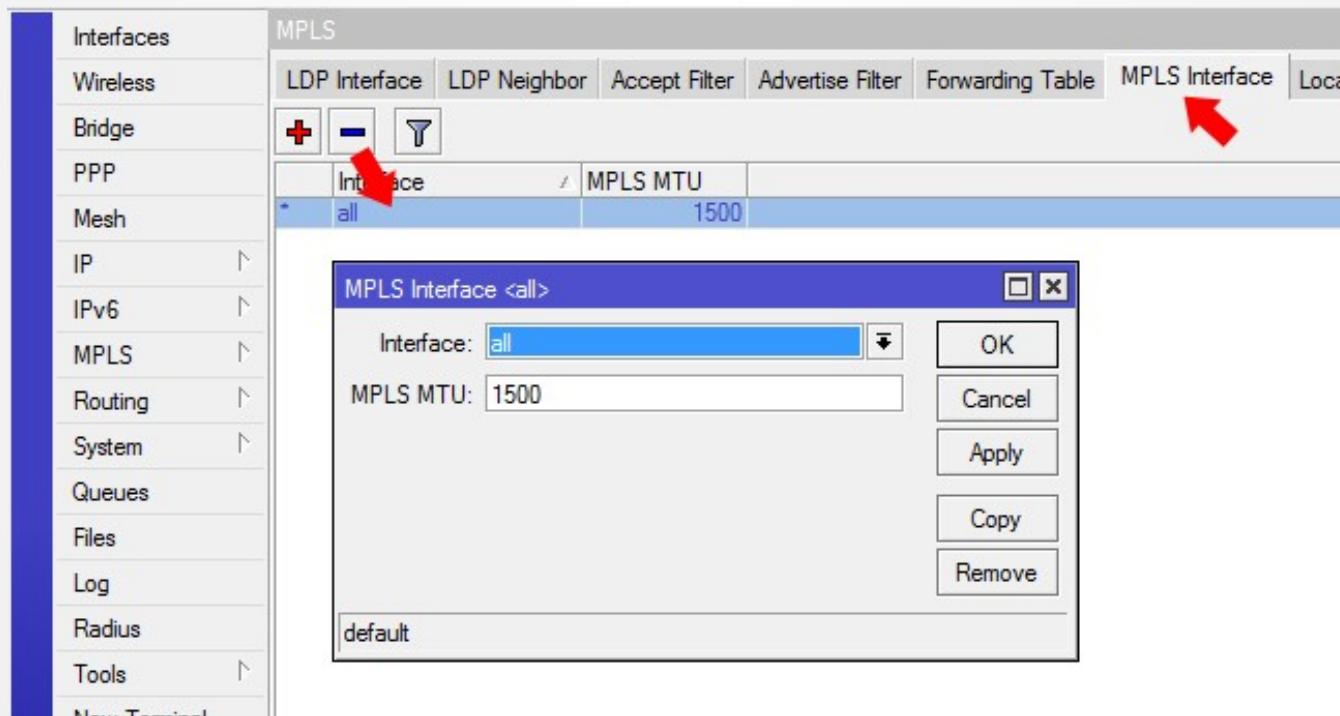
## Configuração – Destino

- \* Menu: MPLS->MPLS;
- \* Acessar LDP Settings selecionar ENABLED;
- \* LSR ID e Transport Address deverá ser o endereço /32 da LOOPBACK;



## Configuração – Destino

- \* Menu: MPLS->MPLS->MPLS Interface;
- \* Todos equipamentos da bridge estão adequados para suportar MTU maior que 1500?



## Configuração – Destino

\* L2MTU

[http://wiki.mikrotik.com/wiki/Manual:Maximum\\_Transmission\\_Unit\\_on\\_RouterBoards](http://wiki.mikrotik.com/wiki/Manual:Maximum_Transmission_Unit_on_RouterBoards)

RouterBoard	MTU description
<b>RB Groove series</b>	ether1:2028
<b>RB Metal series</b>	ether1:2028
<b>RB SXT series</b>	ether1:2028
<b>RB SXT Lite series</b>	ether1:2028
<b>RB SXT G series</b>	ether1:4076
<b>RB750</b>	ether1:4076; ether2-ether5:2028
<b>RB750UP</b>	ether1:4076; ether2-ether5:2028
<b>RB751U-2HnD</b>	ether1:4076; ether2-ether5:2028
<b>RB OmniTik series</b>	ether1:4076; ether2-ether5:2028
<b>RB951-2n</b>	ether1:4076; ether2-ether5:2028
<b>RB951Ui-2HnD</b>	ether1:4076; ether2-ether5:2028
<b>RB750GL</b>	ether1-ether5:4074
<b>RB751G-2HnD</b>	ether1-ether5:4074
<b>RB951G-2HnD</b>	ether1-ether5:4074
<b>RB1200</b>	ether1-ether5:4078, ether6-ether8:4080, ether9-ether10:9116
<b>RB1100AH</b>	ether1-ether10:9498, ether11:, ether12-ether13:9116
<b>RB1100Hx2</b>	ether1-ether10:9498, ether11:9500, ether12-ether13:9116
<b>RB1100AHx2</b>	ether1-ether10:9498, ether11:9500, ether12-ether13:9116
<b>CCR series</b>	ether1-ether12:10226
<b>CRS125-24G-1S</b>	ether1-ether24:4064, sfp1:4064

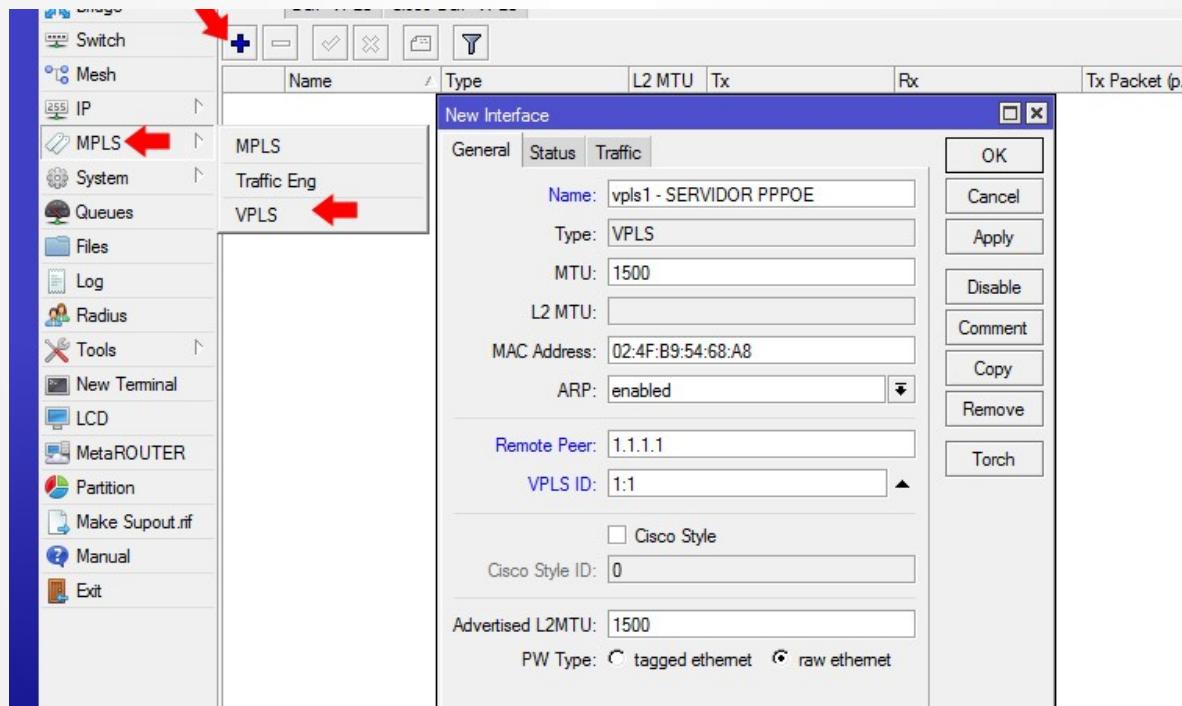
RouterBoard	MTU description
<b>RB411 series</b>	ether1:1526
<b>RB433 series</b>	ether1:1526; ether2-ether3:1522
<b>RB450</b>	ether1:1526; ether2-ether5:1522
<b>RB493 series</b>	ether1:1526; ether2-ether9:1522
<b>RB411GL</b>	ether1:1524
<b>RB433GL</b>	ether1-ether3:1524
<b>RB435G</b>	ether1-ether3:1520
<b>RB450G</b>	ether1-ether5:1520
<b>RB493G</b>	ether1-ether9:1520
<b>RB711 series</b>	ether1:2028
<b>RB711G series</b>	ether1:4076
<b>RB800</b>	ether1-ether2:9500; ether3:9116
<b>RB911G</b>	ether1:4076
<b>RB912UAG</b>	ether1:4076
<b>RB2011 series</b>	ether1-ether5:4074; ether6-ether10:2028; sfp1:4074
<b>RB44Ge</b>	ether1-ether4:9116

RouterBoard	MTU description
<b>RB600 series</b>	ether1-ether3:9500
<b>RB1000</b>	ether1-ether4:9500
<b>RB1100</b>	ether1-ether10:9498; ether11-ether13:9116
<b>RB750G</b>	ether1-ether5:1524

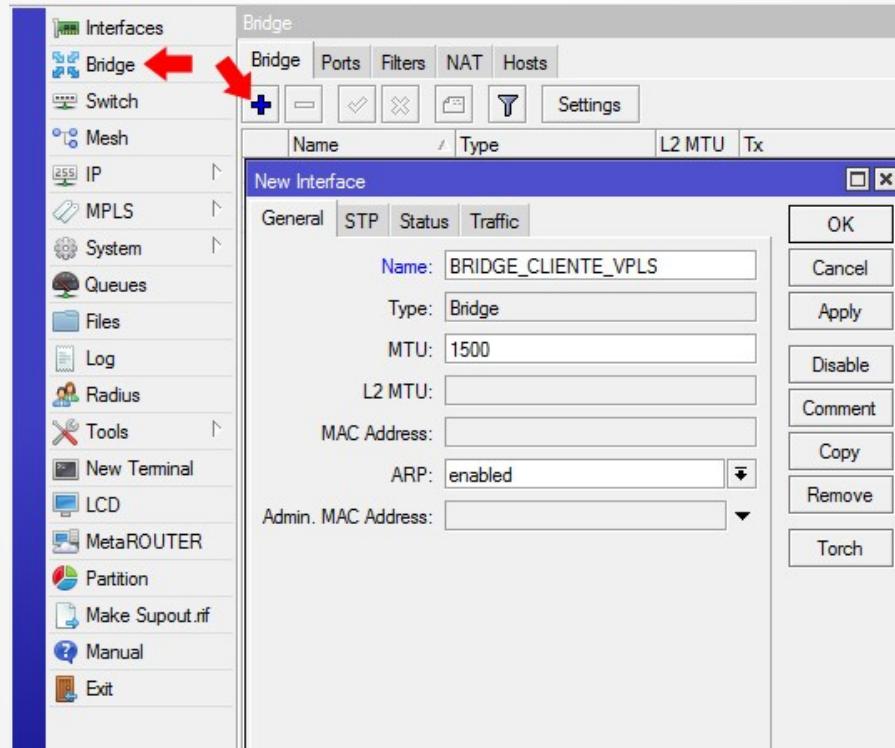
## Configuração – Destino

- \* Menu: MPLS->VPLS;
- \* Adicionar uma nova VPLS com o IP da LOOPBACK do servidor;
- \* Designar o mesmo ID para esse túnel que já foi colocado no servidor;



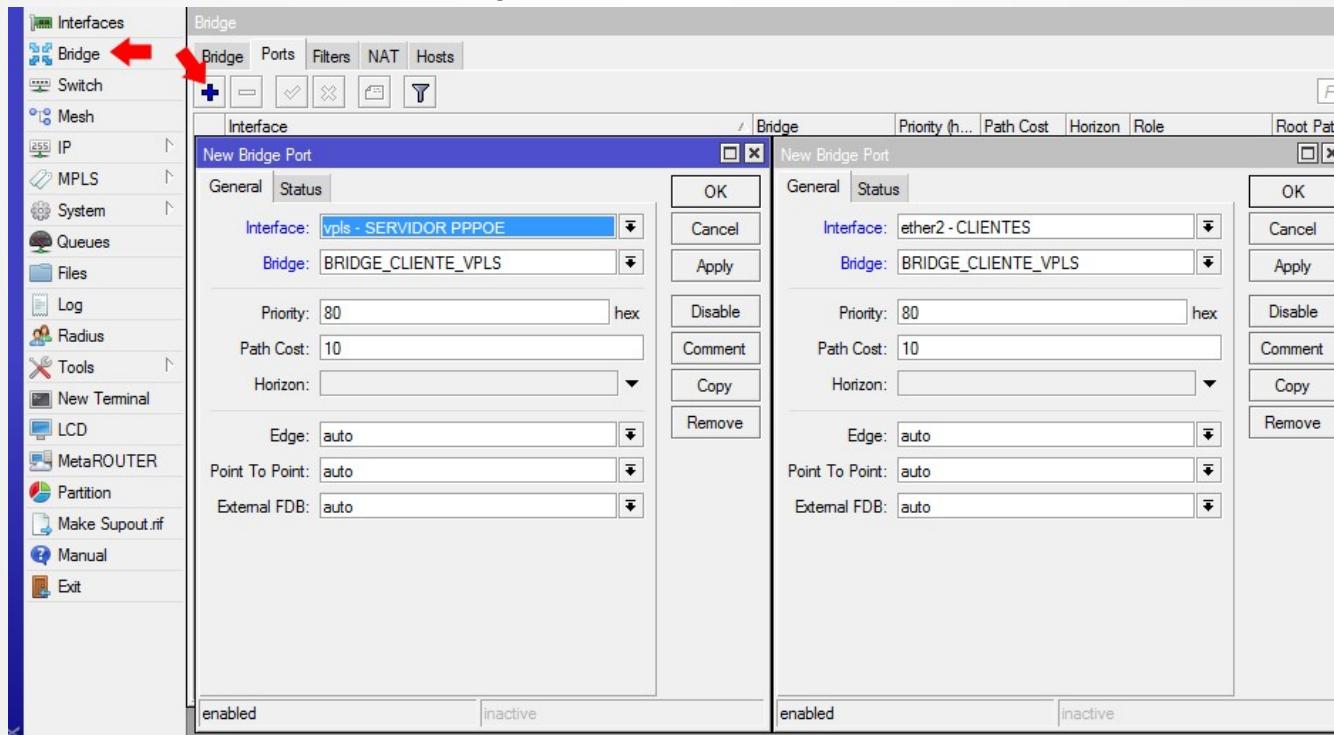
## Configuração – Destino

- \* Menu: Bridge->Bridge;
- \* Adicionar uma nova bridge;



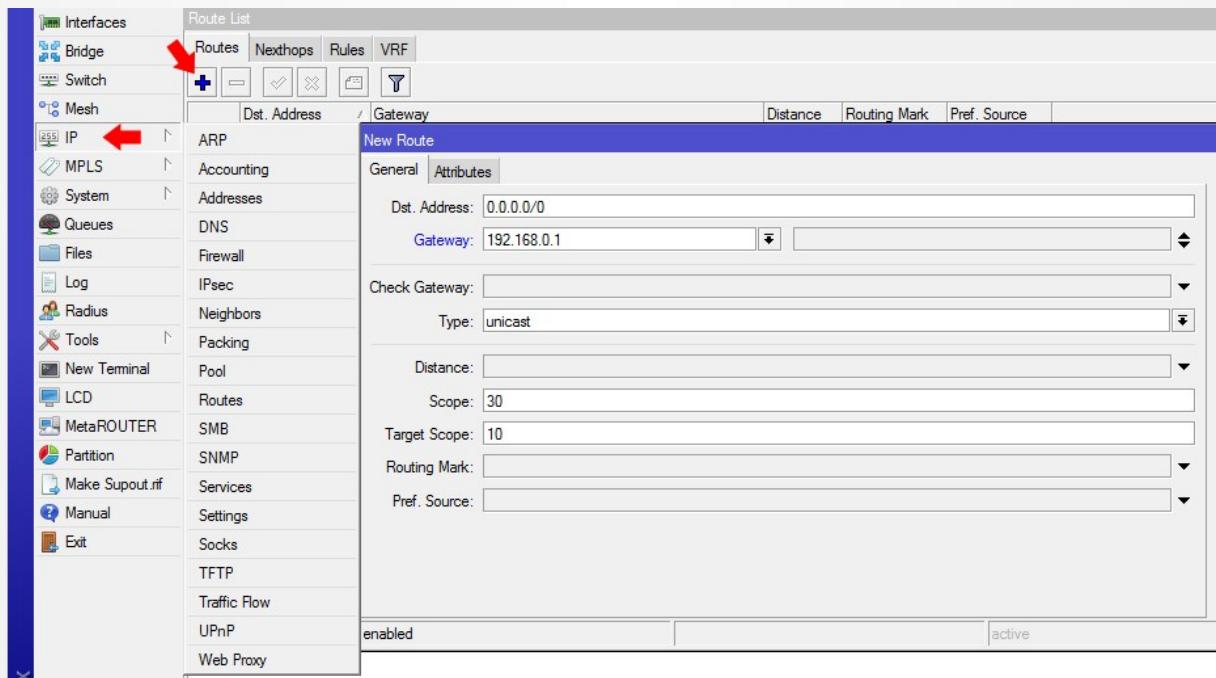
## Configuração – Destino

- \* Menu: Bridge->Ports;
- \* Adicionar a bridge que acabou de ser criada as interfaces onde os clientes estão conectados e juntamente a isso a VPLS criada;



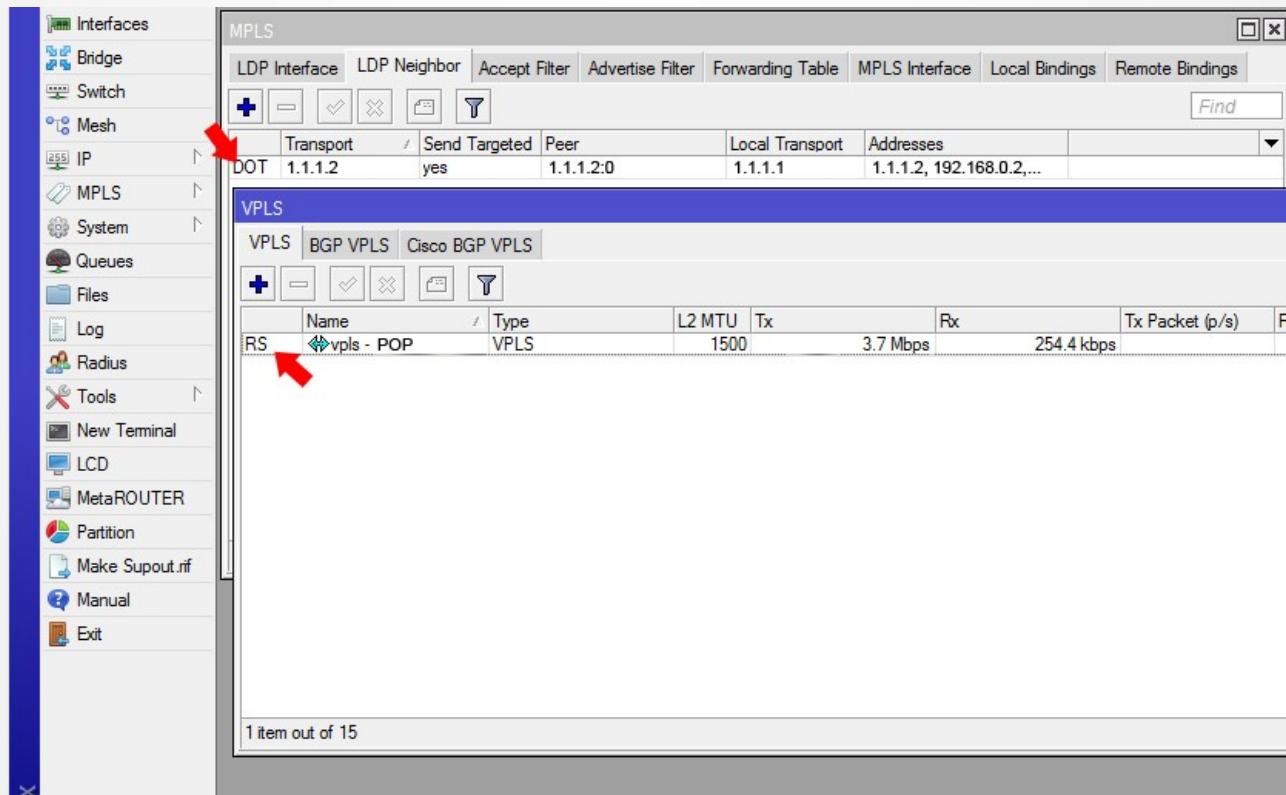
## Configuração – Destino

- \* Menu: IP->Routes;
- \* Adicionar a rota default, caso ela não seja o mesmo servidor que estamos estabelecendo o túnel, informar a rota 1.1.1.1 -> 192.168.0.1;



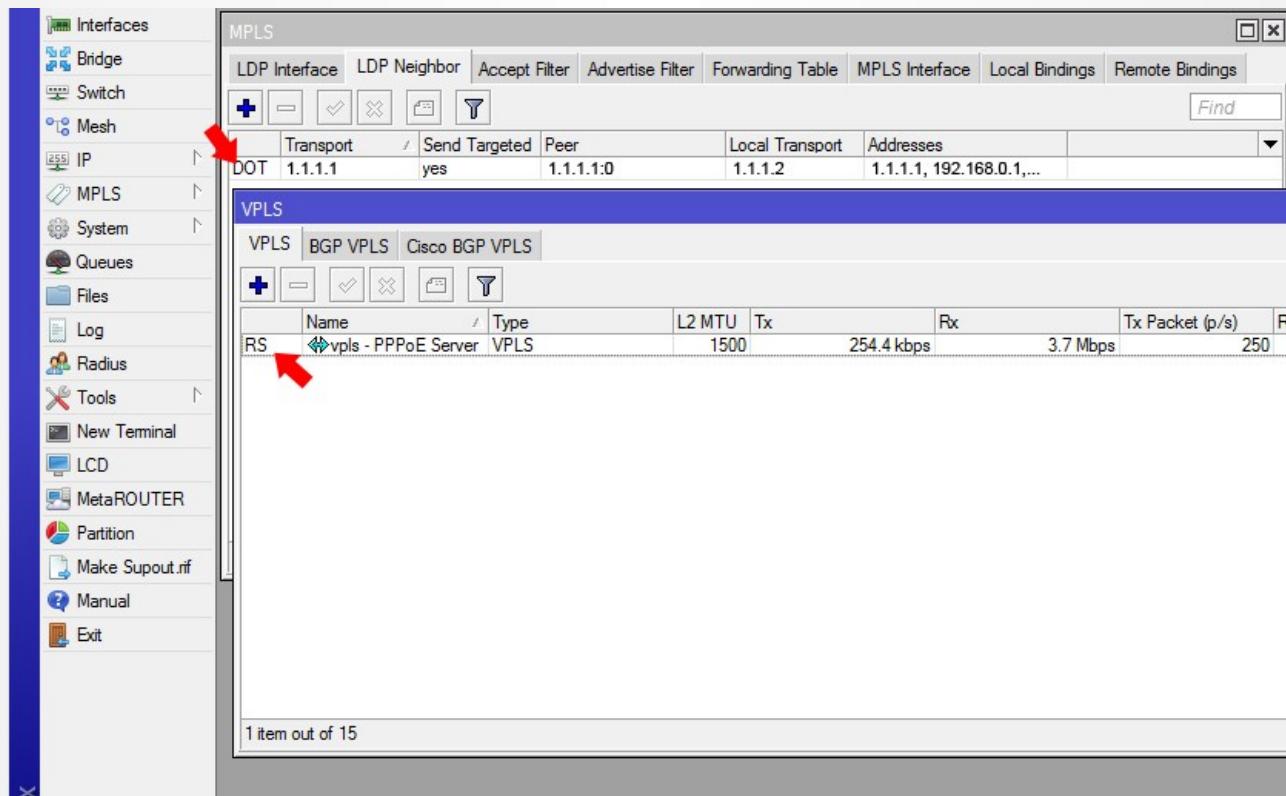
## Verificar – Servidor

\* O túnel deve ter sido estabelecido, vamos verificar;



## Verificar – Destino

\* O túnel deve ter sido estabelecido, vamos verificar;



## Pronto!

Após estas configurações temos a rede com um túnel VPLS sobre MPLS onde os clientes finais somente “veem” o tráfego passante pelo túnel, sendo assim, isolados da estrutura de transporte da rede (core) e de outras células, prédios ou qualquer coisa fora do túnel.

Obs:

O tunelamento só se torna 100% eficiente quando é feito na rede inteira, quem está dentro de um túnel somente prejudica o tráfego daquele túnel! Se existirem clientes diretamente ligados ao core de rede e estes por acaso derem um problema (looping, equipamento com problema, etc.) que seja possível prejudicar o core, irá prejudicar os túneis criados.

**Cliente no core: NÃO!**

Obrigado!

**Eduardo Braum** – Gerente Tecnologia de Informação – (54) 8429-2425  
[eduardo@wavetec.com.br](mailto:eduardo@wavetec.com.br)

**Fernando Klabunde** – Supervisor de Rede – (54) 8429-2429  
[fernandok@wavetec.com.br](mailto:fernandok@wavetec.com.br)