



SERIALLINK VPN

使用说明

SERIALLINK CONFIDENTIAL

目录

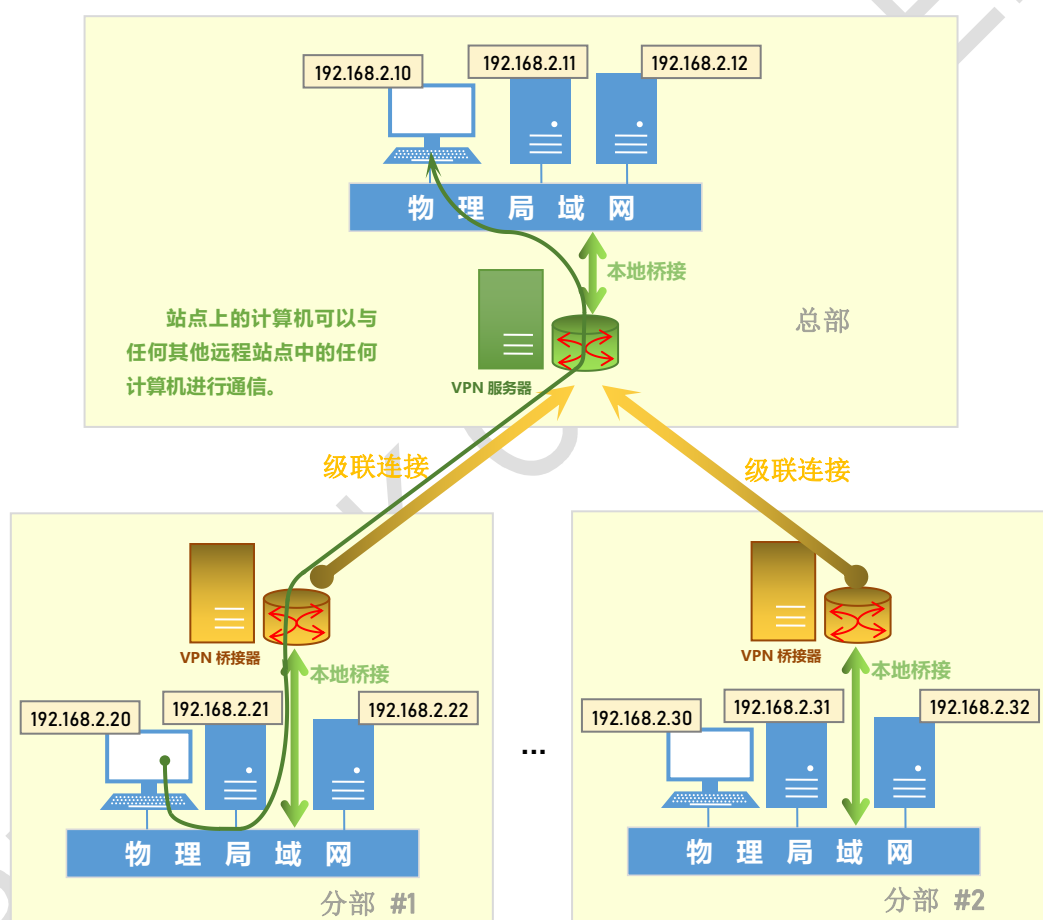
简介.....	3
一、VPN 服务器功能说明.....	4
1.1. 基本配置.....	4
1.2. 高级配置.....	4
二、VPN 桥接器功能说明.....	7
2.1. 基本配置.....	7
2.2. 高级配置.....	7
三、测试实例.....	9
3.1. 配置服务器.....	9
3.2. 配置桥接器.....	11
3.3. 测试结果.....	13

SERIALLINK CONFIDENTIAL

简介

SERIALLINK VPN 虚拟化以太网设备，以便为远程访问 VPN 和站点到站点 VPN 实现灵活的虚拟专用网络。您可以在 SLK-R620（或服务器 PC）上使用 SERIALLINK VPN 建立虚拟 HUB，这台 SLK-R620（或服务器 PC）将成为 VPN 服务器。

然后，您可以在 SLK-R620 上定义两个或多个远程虚拟 HUB 之间的级联连接。通过级联，您可以将两个或多个远程以太网段集成到单个以太网段中。例如，在站点 A、B 和 C 之间建立级联连接后，站点 A 中的任何计算机都可以与站点 B 和站点 C 中的计算机通信。这是站点到站点的 VPN。拓扑图如下：



以下部分介绍如何使用 SERIALLINK VPN 功能。第一、第二章为功能说明，第三章为依照上面拓扑图搭建的测试实例。

一、VPN 服务器功能说明

1.1. 基本配置

此部分描述如何快速配置一个路由器作为 VPN 虚拟局域网中的服务器使用。配置步骤如下：

- ①选择“虚拟专用网”——“SERIALLINK VPN”
- ②勾选“启用”
- ③“服务模式”选择“服务端”
- ④创建一个 HUB，自定义“虚拟 HUB 名”和“HUB 密码”（例：vpntest admin）
- ⑤添加一个用户用于客户端（或者桥接器）验证，自定义“用户名”和“用户密码”（例：user1 slk100200）
- ⑥至此，作为服务器的简单配置完成，点击“保存&应用”即可



1.2. 高级配置

此部分为服务开启时的默认配置，可根据需求自行修改。注意，如果配置不正确，可能导致功能异常。

- ①“管理员密码”：用于通过软件登录 VPN 服务器后台管理的密码，默认 admin



- ②虚拟 NAT 功能：在虚拟 HUB 的虚拟网络上运行一个虚拟 NAT 路由器（IP 伪装）
“开启虚拟 NAT”：勾选开启该功能
“虚拟主机 IP 地址”：服务器在虚拟网络中的 IP 地址，默认 192.168.30.1
“子网掩码”：服务器的子网掩码，默认 255.255.255.0

开启虚拟NAT <input checked="" type="checkbox"/>	启用虚拟NAT功能
虚拟主机IP地址	<input type="text" value="192.168.30.1"/>
	指定虚拟接口的IP地址
子网掩码	<input type="text" value="255.255.255.0"/>
	指定虚拟接口的子网掩码

③DHCP 服务器功能：在虚拟网络中推送至客户端的 IP 地址池

“开启 DHCP”：勾选开启该功能

“起始 IP 地址”：从该地址开始为接入客户端分配 IP，默认 192.168.30.10

“终止 IP 地址”：为客户端分配 IP 地址至该地址，默认 192.168.30.200，即分配给客户端的 IP 地址范围在 192.168.30.10~192.168.30.200

“子网掩码”：客户端的子网掩码，默认 255.255.255.0

“租赁期限”：在服务器为客户端分配 IP 地址满的情况下，当存在新的客户端接入，到期的 IP 地址将被释放以分配给新的客户端，单位：秒

“网关”：推送至客户端的默认网关，默认虚拟主机 IP 地址

“DNS”：推送至客户端的主 DNS 服务器的 IP 地址，默认 192.168.30.1

开启DHCP <input checked="" type="checkbox"/>	启用虚拟DHCP服务器功能
起始IP地址	<input type="text" value="192.168.30.10"/>
	指定要分发给客户端的地址范围的起始IP地址(例如: 192.168.30.10)
终止IP地址	<input type="text" value="192.168.30.200"/>
	指定要分发给客户端的地址范围的终止IP地址(例如: 192.168.30.200)
子网掩码	<input type="text" value="255.255.255.0"/>
	为客户端指定子网掩码
租赁期限	<input type="text" value="7200"/>
	以秒为单位指定将IP地址租给客户端的到期日期
网关	<input type="text" value="192.168.30.1"/>
	指定推送至客户端的默认网关的IP地址
DNS	<input type="text" value="192.168.30.1"/>
	指定推送至客户端的主DNS服务器的IP地址

④ “本地网桥”：作为服务器，需要选择一个网络接口用于客户端或桥接器进行虚拟局域网通讯



本地网桥 br-lan

启用本地网桥

Tap设备

使用新Tap设备的桥接

⑤ “Tap 设备”：当创建一个新的网络接口作为本地网桥而不是选择已存在的网络接口时，需要勾选。

⑥ “禁用页面配置”：仅需要运行服务器，而不需要通过页面的方式配置，勾选该功能。而后可通过软件登录服务器后台管理作进一步的配置

二、VPN 桥接器功能说明

2.1. 基本配置

此部分描述如何快速配置一个路由器作为 VPN 虚拟局域网中的桥接器使用。配置步骤如下：

- ①选择“虚拟专用网”——“SERIALLINK VPN”
- ②勾选“启用”
- ③“服务模式”选择“桥接”
- ④创建一个级联连接连接服务器，自定义“级联连接名”（例：`conn2`）
- ⑤“主机名”填写 VPN 服务器的公网 IP（或解析了公网 IP 的域名）
- ⑥“端口”填写 VPN 服务器的端口号（说明：VPN 服务器默认允许 `443`，`992`，`1194`，`5555` 端口接入，例：`5555`）
- ⑦“虚拟 HUB 名”填写远程接入 VPN 服务器的虚拟 HUB 名（由 VPN 服务器提供）
- ⑧填写用于验证接入 VPN 服务器的“用户名”和“密码”（由 VPN 服务器提供）
- ⑨至此，作为桥接器的简单配置完成，点击“保存&应用”



2.2. 高级配置

此部分为服务开启时的默认配置，可根据需求自行修改。注意，如果配置不正确，可能导致功能异常。

- ①“管理员密码”：用于通过软件登录 VPN 服务器后台管理的密码，默认 `admin`
- ②“本地网桥”：作为桥接器，默认选择 `br-lan`



③ “Tap 设备”：当创建一个新的网络接口作为本地网桥而不是选择已存在的网络接口时，需要勾选。

④ “禁用页面配置”：仅需要运行桥接器，而不需要通过页面的方式配置，勾选该功能。而后可通过软件登录桥接器后台管理作进一步的配置

三、测试实例

此部分按照拓扑图使用三台 **slk-r620** 进行配置测试，其中一台 IP 地址 **192.168.2.1** 作为 VPN 服务器（下接计算机 **192.168.2.10**）；另外两台 IP 地址 **192.168.2.2**（下接计算机 **192.168.2.20**）和 **192.168.2.3**（下接计算机 **192.168.2.30**）作为 VPN 桥接器。所有计算机的网关改为其上级 **SLK-R620** 的 IP 地址，例如 **192.168.2.10** 的计算机网关为 **192.168.2.1**；**192.168.2.20** 的计算机网关为 **192.168.2.2**。并且计算机需要关闭防火墙。

3.1. 配置服务器

参考 1.1，只需要基本配置 **SLK-R620** 即可以建立一个 VPN 服务器，**192.168.2.1** 配置如下：

① “服务模式” 选择 “服务端”

② 自定义一个新的 “虚拟 HUB 名”，例： **vpntest**

③ 为第②中的虚拟 HUB 设置 “HUB 密码”，例： **admin**

④ 创建一个新用户（用于 VPN 桥接器等远程站点接入服务时的身份验证），自定义 “用户名”，例： **user1**

⑤ 为④中的用户设置 “用户密码”，例： **slk100200**

基本设置	高级设置
启用 <input checked="" type="checkbox"/>	
服务模式	服务端
选择VPN服务模式	
虚拟HUB名	vpntest
指定要创建的虚拟HUB的名称	
HUB密码
为创建的虚拟HUB设置管理员密码	
用户名	user1
指定新建用户的用户名	
用户密码
指定要为该用户设置的密码	

高级配置部分保留了默认配置，无需修改。特别的，本测试实例 VPN 服务器有下接设备 192.168.2.10 需要和其他远程站点的下接设备 192.168.2.20 和 192.168.2.30 远程通讯，“本地网桥”选择 br-lan；若 VPN 服务器仅有 eth0 网络接口，且无下接设备，应创建一个新的本地网桥，并勾选“Tap 设备”

基本设置	高级设置
管理员密码	<input type="password" value="....."/>  设置VPN服务器管理员密码
开启虚拟NAT	<input checked="" type="checkbox"/> 启用虚拟NAT功能
虚拟主机IP地址	<input type="text" value="192.168.30.1"/> 指定虚拟接口的IP地址
子网掩码	<input type="text" value="255.255.255.0"/>  指定虚拟接口的子网掩码
开启DHCP	<input checked="" type="checkbox"/> 启用虚拟DHCP服务器功能
起始IP地址	<input type="text" value="192.168.30.10"/> 指定要分发给客户端的地址范围的起始IP地址(例如: 192.168.30.10)
终止IP地址	<input type="text" value="192.168.30.200"/> 指定要分发给客户端的地址范围的终止IP地址(例如: 192.168.30.200)
子网掩码	<input type="text" value="255.255.255.0"/>  为客户端指定子网掩码
租赁期限	<input type="text" value="7200"/> 以秒为单位指定将IP地址租给客户端的到期日期
网关	<input type="text" value="192.168.30.1"/> 指定推送至客户端的默认网关的IP地址
DNS	<input type="text" value="192.168.30.1"/> 指定推送至客户端的主DNS服务器的IP地址
本地网桥	 br-lan  启用本地网桥
Tap设备	<input type="checkbox"/> 使用新Tap设备的桥接
禁用页面配置	<input type="checkbox"/> 仅开启VPN服务并关闭页面配置功能

3.2. 配置桥接器

1) 参考 2.1，基本配置另外两台 SLK-R620 作为 VPN 桥接器。192.168.2.2 配置如下：

① “服务模式”选择“桥接”

② 自定义一个“级联连接名”，例：**bridgeconn1**

③ 填写“主机名”，注：想要获得远程通讯，“主机名”需要填写一个公网 IP 或解析了公网 IP 的域名。这里填写 **183.15.121.150** 实际为 **192.168.2.1**（VPN 服务器）的公网 IP 地址。

④ 填写“端口”，注：**192.168.2.1**（VPN 服务器）默认开放 **443,992,555,8888** 四个端口供桥接器远程接入服务（需要确保 **192.168.2.1** 上这些端口没有被其他服务占用）。此实例中，我们将 **192.168.2.1** 的 TCP 端口 **443** 通过防火墙映射到 **183.15.124.150** 的端口 **6621**。

⑤ 指定“虚拟 HUB 名”，例：**vpntest**（即 **192.168.2.1** 中创建的虚拟 HUB 名）


⑥ 指定“用户名”和“用户密码”用于本地站点远程接入 VPN 服务器时验证用户身份（即 **192.168.2.1** 中添加的用户）

基本设置		高级设置	
启用 <input checked="" type="checkbox"/>			
服务模式	桥接	选择VPN服务模式	
级联连接名	bridgeconn1	指定要创建的级联连接的名称	
主机名	183.15.121.150	指定目标VPN服务器的主机名	
端口	6621	指定目标VPN服务器的端口号	
虚拟HUB名	vpntest	指定目标VPN服务器上的虚拟HUB	
用户名	user1	指定连接到目标VPN服务器时用于用户验证的用户名	
用户密码	指定用于密码验证的密码	

高级配置保持默认，不作修改。

基本设置	高级设置
管理员密码 
设置VPN桥接器管理员密码	
本地网桥	 br-lan
启用本地网桥	
Tap设备	<input type="checkbox"/>
使用新Tap设备的桥接	
禁用页面配置	<input type="checkbox"/>
仅开启VPN服务并关闭页面配置功能	

2) 192.168.2.3 配置如下:

基本设置	高级设置
启用	<input checked="" type="checkbox"/>
服务模式	桥接
选择VPN服务模式	
级联连接名	bridgeconn2
指定要创建的级联连接的名称	
主机名	183.15.121.150
指定目标VPN服务器的主机名	
端口	6621
指定目标VPN服务器的端口号	
虚拟HUB名	vpntest
指定目标VPN服务器上的虚拟HUB	
用户名	user1
指定连接到目标VPN服务器时用于用户验证的用户名	
用户密码 
指定用于密码验证的密码	

基本设置	高级设置
管理员密码 
设置VPN桥接器管理员密码	
本地网桥	 br-lan
启用本地网桥	
Tap设备	<input type="checkbox"/>
使用新Tap设备的桥接	
禁用页面配置	<input type="checkbox"/>
仅开启VPN服务并关闭页面配置功能	

3.3. 测试结果

如拓扑图所示，总部 SLK-R620 地址 192.168.2.1，下接计算机地址 192.168.2.10；分部#1 SLK-R620 地址 192.168.2.2，下接计算机地址 192.168.2.20；分部#2 SLK-R620 地址 192.168.2.3，下接计算机地址 192.168.2.30

1) 总部 ping 分部

①192.168.2.10 ping 192.168.2.20

```
来自 192.168.2.20 的回复: 字节=32 时间=79ms TTL=64
来自 192.168.2.20 的回复: 字节=32 时间=51ms TTL=64
来自 192.168.2.20 的回复: 字节=32 时间=49ms TTL=64
来自 192.168.2.20 的回复: 字节=32 时间=49ms TTL=64
来自 192.168.2.20 的回复: 字节=32 时间=70ms TTL=64
来自 192.168.2.20 的回复: 字节=32 时间=46ms TTL=64
来自 192.168.2.20 的回复: 字节=32 时间=47ms TTL=64
来自 192.168.2.20 的回复: 字节=32 时间=50ms TTL=64
```

192.168.2.20 的 Ping 统计信息:

数据包: 已发送 = 2893, 已接收 = 2882, 丢失 = 11 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 29ms, 最长 = 3698ms, 平均 = 71ms

②192.168.2.10 ping 192.168.2.30

```
来自 192.168.2.30 的回复: 字节=32 时间=595ms TTL=64
来自 192.168.2.30 的回复: 字节=32 时间=513ms TTL=64
来自 192.168.2.30 的回复: 字节=32 时间=37ms TTL=64
来自 192.168.2.30 的回复: 字节=32 时间=62ms TTL=64
来自 192.168.2.30 的回复: 字节=32 时间=45ms TTL=64
来自 192.168.2.30 的回复: 字节=32 时间=777ms TTL=64
来自 192.168.2.30 的回复: 字节=32 时间=40ms TTL=64
来自 192.168.2.30 的回复: 字节=32 时间=37ms TTL=64
```

192.168.2.30 的 Ping 统计信息:

数据包: 已发送 = 2338, 已接收 = 2338, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 28ms, 最长 = 777ms, 平均 = 61ms

2) 分部 ping 总部

①192.168.2.20 ping 192.168.2.10

```
来自 192.168.2.10 的回复: 字节=32 时间=51ms TTL=64
来自 192.168.2.10 的回复: 字节=32 时间=58ms TTL=64
来自 192.168.2.10 的回复: 字节=32 时间=54ms TTL=64
来自 192.168.2.10 的回复: 字节=32 时间=62ms TTL=64
来自 192.168.2.10 的回复: 字节=32 时间=39ms TTL=64
来自 192.168.2.10 的回复: 字节=32 时间=49ms TTL=64
来自 192.168.2.10 的回复: 字节=32 时间=62ms TTL=64
来自 192.168.2.10 的回复: 字节=32 时间=45ms TTL=64
```

192.168.2.10 的 Ping 统计信息:

数据包: 已发送 = 1415, 已接收 = 1412, 丢失 = 3 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 29ms, 最长 = 3574ms, 平均 = 83ms

②192.168.2.30 ping 192.168.2.10

```
来自 192.168.2.10 的回复: 字节=32 时间=44ms TTL=64
来自 192.168.2.10 的回复: 字节=32 时间=40ms TTL=64
来自 192.168.2.10 的回复: 字节=32 时间=39ms TTL=64
来自 192.168.2.10 的回复: 字节=32 时间=44ms TTL=64
来自 192.168.2.10 的回复: 字节=32 时间=55ms TTL=64
来自 192.168.2.10 的回复: 字节=32 时间=42ms TTL=64
来自 192.168.2.10 的回复: 字节=32 时间=45ms TTL=64
来自 192.168.2.10 的回复: 字节=32 时间=72ms TTL=64
```

```
192.168.2.10 的 Ping 统计信息:
数据包: 已发送 = 5061, 已接收 = 5060, 丢失 = 1 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 28ms, 最长 = 1334ms, 平均 = 49ms
```

3) 分部 ping 分部

①192.168.2.20 ping 192.168.2.30

```
来自 192.168.2.30 的回复: 字节=32 时间=85ms TTL=64
来自 192.168.2.30 的回复: 字节=32 时间=77ms TTL=64
来自 192.168.2.30 的回复: 字节=32 时间=91ms TTL=64
来自 192.168.2.30 的回复: 字节=32 时间=184ms TTL=64
来自 192.168.2.30 的回复: 字节=32 时间=81ms TTL=64
来自 192.168.2.30 的回复: 字节=32 时间=95ms TTL=64
来自 192.168.2.30 的回复: 字节=32 时间=182ms TTL=64
来自 192.168.2.30 的回复: 字节=32 时间=90ms TTL=64
```

```
192.168.2.30 的 Ping 统计信息:
数据包: 已发送 = 1660, 已接收 = 1660, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 58ms, 最长 = 955ms, 平均 = 106ms
```

②192.168.2.30 ping 192.168.2.20

```
来自 192.168.2.20 的回复: 字节=32 时间=107ms TTL=64
来自 192.168.2.20 的回复: 字节=32 时间=101ms TTL=64
来自 192.168.2.20 的回复: 字节=32 时间=97ms TTL=64
来自 192.168.2.20 的回复: 字节=32 时间=74ms TTL=64
来自 192.168.2.20 的回复: 字节=32 时间=110ms TTL=64
来自 192.168.2.20 的回复: 字节=32 时间=88ms TTL=64
来自 192.168.2.20 的回复: 字节=32 时间=85ms TTL=64
来自 192.168.2.20 的回复: 字节=32 时间=101ms TTL=64
```

```
192.168.2.20 的 Ping 统计信息:
数据包: 已发送 = 2343, 已接收 = 2341, 丢失 = 2 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 58ms, 最长 = 1109ms, 平均 = 97ms
```

感谢您对赛诺联克产品的支持。

若您有任何问题，可联系邮箱: info@seriallink.net 或登陆官网: www.seriallink.net

SERIAL LINK CONFIDENTIAL