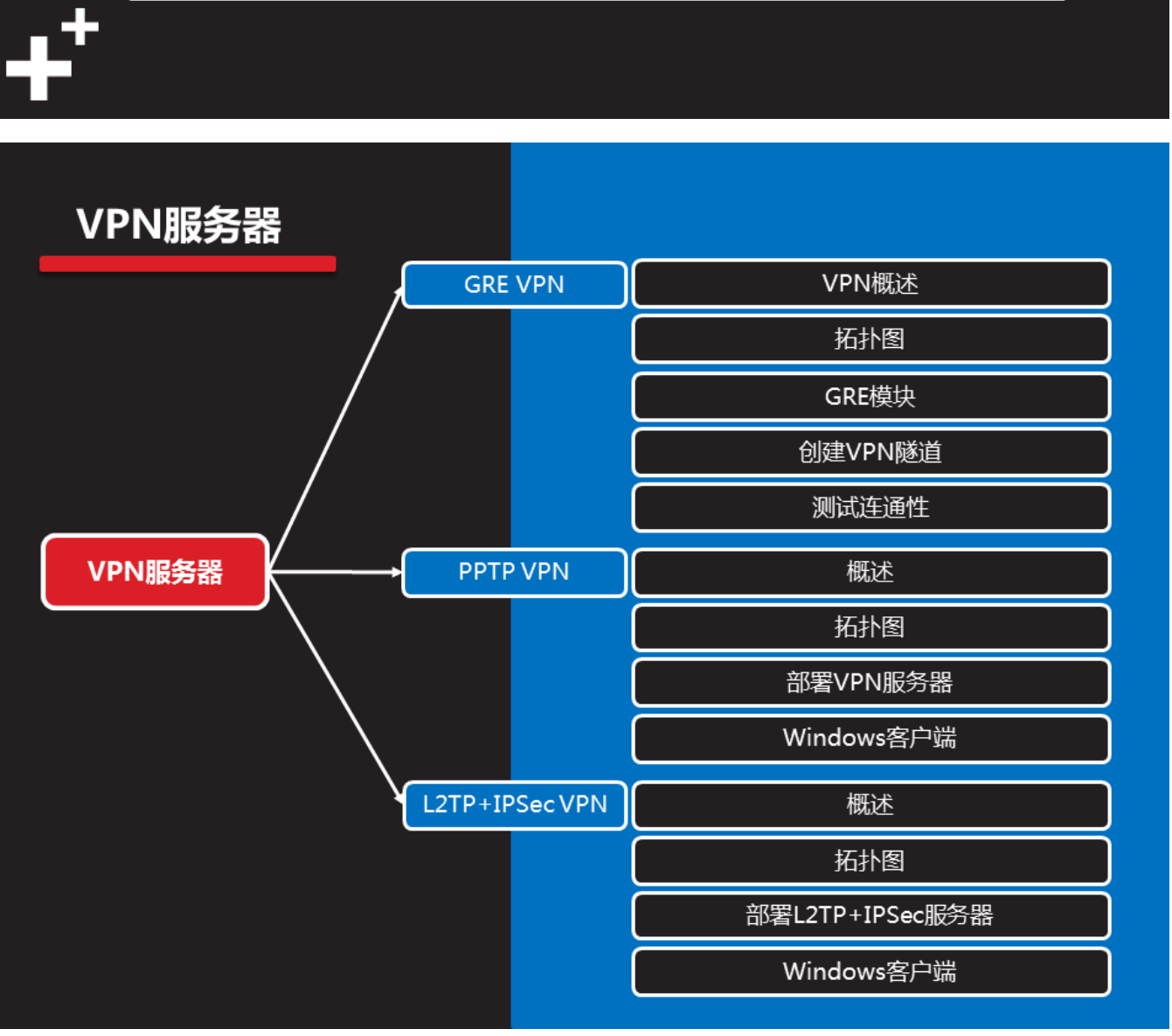
OPERATION DAY07

内容

上午	09:00 ~ 09:30	作业讲解和回顾
	09:30 ~ 10:20	VPN服务器
	10:30 ~ 11:20	
	11:30 ~ 12:20	
下午	14:00 ~ 14:50	
	15:00 ~ 15:50	NTP时间同步
	16:00 ~ 16:50	PSSH远程工具
	17:00 ~ 17:30	总结和答疑



GRE VPN

VPN概述

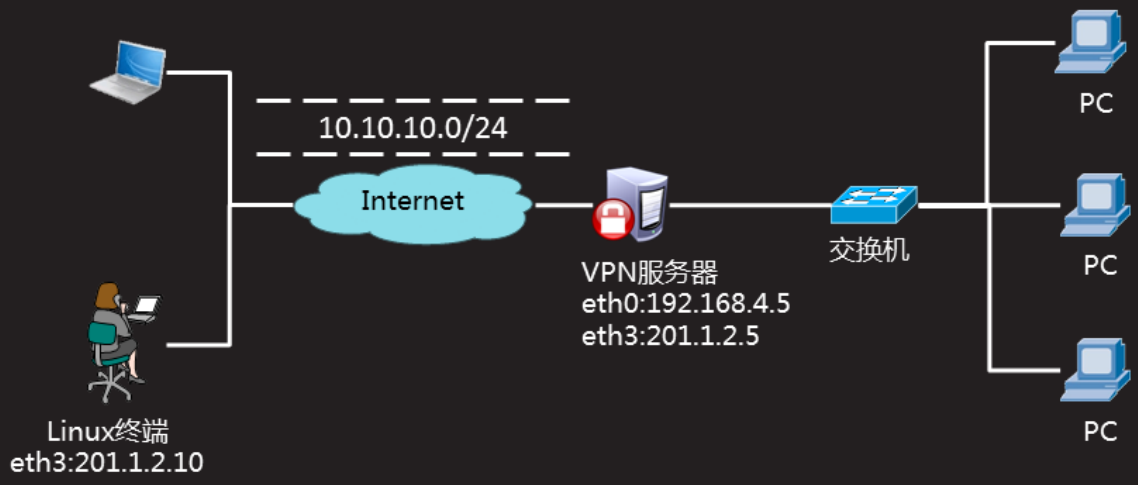
知识讲解

- Virtual Private Network（虚拟专用网络）
  - 在公用网络上建立专用私有网络，进行加密通讯
  - 多用于为集团公司的各地子公司建立连接
  - 连接完成后，各个地区的子公司可以像局域网一样通讯
  - 在企业网络中有广泛应用
  - 偶尔可以用于翻墙
  - 目前主流的VPN技术（GRE，PPTP，L2TP+IPSec，SSL）

拓扑图

知识讲解

- 出差在外，连接公司的服务器
- 或者，分公司之间的连接



GRE模块

知识讲解

- Linux内核模块
  - ip_gre
- 加载模块
  - lsmod | grep ip_gre //显示模块列表
  - modprobe ip_gre //加载模板
  - modinfo ip_gre //查看模块信息
- 缺点：缺少加密机制

创建VPN隧道

Tedu.cn 达内教育

知识讲解

- Client

```
[root@clinet ~]# modprobe ip_gre
[root@client ~]# ip tunnel add tun0 mode gre \
> remote 201.1.2.5 local 201.1.2.10
[root@client ~]# ip link set tun0 up
[root@client ~]# ip addr add 10.10.10.10/24 peer 10.10.10.5/24 \
> dev tun0
[root@client ~]# firewall-cmd --set-default-zone=trusted
```

创建VPN隧道（续1）

Tedu.cn 达内教育

知识讲解

- VPN服务器

```
[root@proxy ~]# modprobe ip_gre
[root@proxy ~]# ip tunnel add tun0 mode gre \
> remote 201.1.2.10 local 201.1.2.5
[root@proxy ~]# ip link set tun0 up
[root@proxy ~]# ip addr add 10.10.10.5/24 peer 10.10.10.10/24 \
> dev tun0
[root@proxy ~]# echo "1" > /proc/sys/net/ipv4/ip_forward
[root@proxy ~]# firewall-cmd --set-default-zone=trusted
```

测试连通性

知识讲解

- Client

```
[root@client ~]#  ping 10.10.10.5
[root@client ~]#  ping 192.168.4.5
```

- Proxy

```
[root@proxy ~]#  ping 10.10.10.10
```

案例1：配置GRE VPN

课堂练习

- 启用内核模块ip_gre
- 创建一个虚拟VPN隧道(10.10.10.0/24)
- 实现两台主机点到点的隧道通讯

PPTP VPN

概述

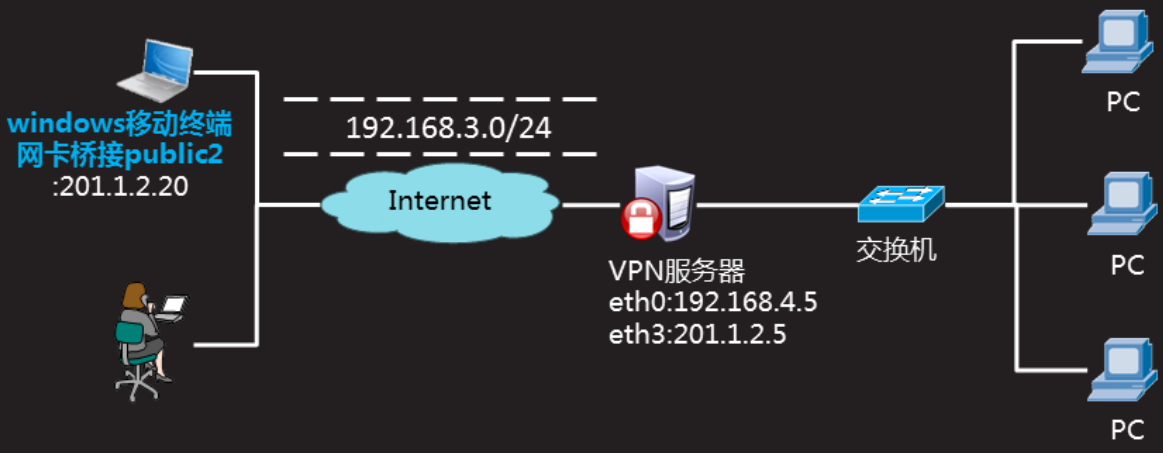
知识讲解

- PPTP（Point to Point Tunneling Protocol）
- 支持密码身份验证
- 支持MPPE(Microsoft Point-to-Point Encryption)加密

拓扑图

知识讲解

- 拓扑图沿用之前实验的拓扑结构
- 使用一台Windows主机做为客户端
- Windows IP地址为:201.1.2.20/24



部署VPN服务器

知识讲解

- 安装软件

```
[root@proxy ~]#  yum localinstall pptpd-1.4.0-2.el7.x86_64.rpm
[root@proxy ~]#  rpm -qc pptpd
/etc/ppp/options.pptpd
/etc/pptpd.conf
/etc/sysconfig/pptpd
```

部署VPN服务器（续1）

知识讲解

- 修改配置文件

```
[root@proxy ~]#  vim /etc/pptpd.conf
localip 201.1.2.5                          //服务器本地IP
remoteip 192.168.3.1-50                    //分配给客户端的IP池

[root@proxy ~]#  vim /etc/ppp/options.pptpd
require-mppe-128                           //使用MPPE加密数据
ms-dns 8.8.8.8                             //DNS服务器

[root@proxy ~]#  vim /etc/ppp/chap-secrets
jacob           *              123456          *
//用户名        服务器标记     密码     客户端

[root@proxy ~]#  echo "1" > /proc/sys/net/ipv4/ip_forward
```

部署VPN服务器（续2）

知识讲解

- 启动服务

```
[root@proxy ~]# systemctl start pptpd
[root@proxy ~]# firewall-cmd --set-default-zone=trusted
```

- 翻墙设置

```
[root@proxy ~]# iptables -t nat -A POSTROUTING -s 192.168.3.0/24 \
>  -j SNAT --to-source 201.1.2.5
```

Tedu.cn

Windows客户端（续1）

Tedu.cn 达内教育

- 测试

知

案例2：创建PPTP VPN

课堂练习

- 使用PPTP协议创建一个支持身份验证的隧道连接
- 使用MPPE对数据进行加密
- 为客户端分配192.168.3.0/24的地址池
- 客户端连接的用户名为jacob，密码为123456

L2TP+IPSec VPN

概述

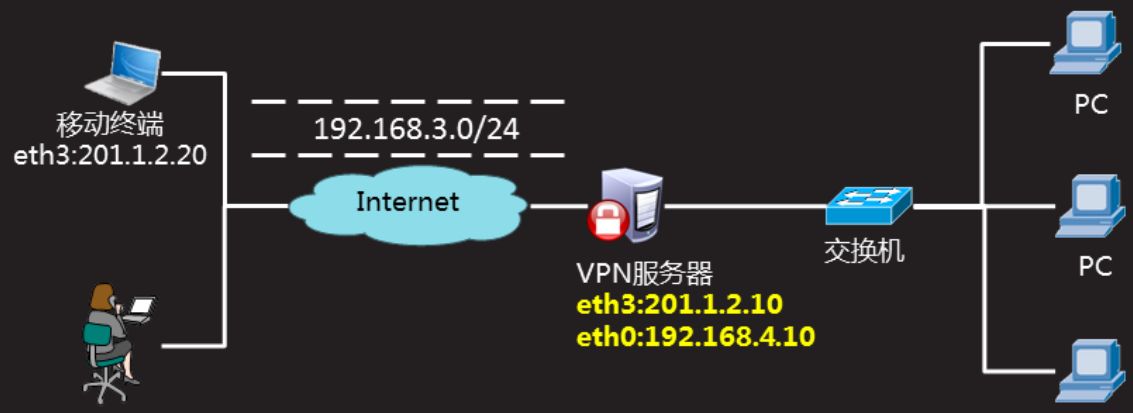
知识讲解

- Layer Two Tunneling Protocol（L2TP）
- L2TP建立主机之间的VPN隧道，压缩、验证
- IPSec提供数据加密、数据校验、访问控制的功能

拓扑图

知识讲解

- 沿用之前实验的拓扑结构
- 使用另一台VPN服务器，配置IP地址



部署L2TP+IPSec服务器

Tedu.cn 达内教育

知识讲解

- 安装软件

```
[root@vpn ~]# yum -y install libreswan
[root@vpn ~]# yum localinstall xl2tpd-1.3.8-2.el7.x86_64.rpm
```

部署L2TP+IPSec服务器（续1）

Tedu.cn 达内教育

知识讲解

- 创建IPSec加密配置文件

```
[root@vpn ~]#  vim /etc/ipsec.d/myipsec.conf          //新建文件
conn IDC-PSK-NAT
  rightsubnet=vhost:%priv                             //允许的VPN虚拟网络
  also=IDC-PSK-noNAT

conn IDC-PSK-noNAT
  authby=secret                                       //加密认证
    ike=3des-sha1;modp1024                            //算法
    phase2alg=aes256-sha1;modp2048                    //算法
  pfs=no
  auto=add
  keyingtries=3
  rekey=no
  ikelifetime=8h
  keylife=3h
  type=transport
  left=201.1.2.10                                     //重要，服务器本机的外网IP
  leftprotoport=17/1701
  right=%any                                          //允许任何客户端连接
  rightprotoport=17/%any
```

部署L2TP+IPSec服务器（续3）

Tedu.cn 达内教育

知识讲解

- 启动IPSec服务

```
[root@vpn ~]#  systemctl start ipsec

[root@vpn ~]# netstat -ntulp |grep pluto
```