VPN技术的“集大成”者——动态多点VPN

思科社区【公开课】第四十四期

徐宇斌

上海桓文教育创始人 资深CCIE培训讲师

2019.01.16

会议日程_思科社区公开课

会议时间：2019年01月16日 星期三 10:00-12:00

会议主题：VPN技术的“集大成”者——动态多点VPN

演讲嘉宾：徐宇斌

徐宇斌 上海桓文教育 **创始人**
资深 CCIE 培训讲师 | CCIE R&S / Security

多年来一直从事网络安全方面的研究，多次发表论文专著，是上个世纪九十年代我国自己培养起来的**第一代网络安全专家**。

从 2000 年起开始涉足 Cisco 认证考试领域，多年来，积累了丰富的 Cisco 认证考试教学经验，是中国大陆 IT 培训界**资深的 CCIE 培训讲师**。

- 毕业于清华大学计算机系计算机网络专业
- 路由交换、网络安全双 CCIE
- Cisco 授权 CCSI 讲师

演讲过程中，如果您有问题，可以在“问与答”窗口进行 文字提问，我们的专家会尽量为您解答。

Agenda/目录

- 讲师自我介绍
- VPN技术的起源
- 传统VPN技术在使用中所面临的问题
- 动态多点VPN“集大成”
- DMVPN的思科设备实现（实验演示）
- Q & A

初出茅庐 风华正茂

退居二线 传承思科

上海桓文教育　　www.huanwen.net

思科培训 请认准思科授权机构

cisco

Cisco Learning
Partner Program

Cisco Learning Partner

Awarded to
SHANGHAI HUANWEN EDUCATION INFORMATION CONSULATION COMPANY LTD

cisco
Learning
Partner

Delivery Area
CHINA
valid until 24-OCT-2019

Validate this certificate at:
cisco.com/go/partnerlocator

Kamal Lamba
Global Partner Manager

This certificate acknowledges that this partner is authorized to deliver Cisco training.

思科培训 请认准思科授权讲师

Cisco Certifications

Yu Bin Xu

has successfully completed the Cisco certification exam requirements and is recognized as a

Certified Cisco Systems Instructor

CISCO CERTIFIED CCSI INSTRUCTOR

Date Certified: 06/02/2010
Valid through: 08/02/2019
CCSI ID: 33518
Cisco ID: CSCO10204228

Chuck Robbins
Chief Executive Officer
Cisco Systems, Inc.

思科授权教育培训合作伙伴

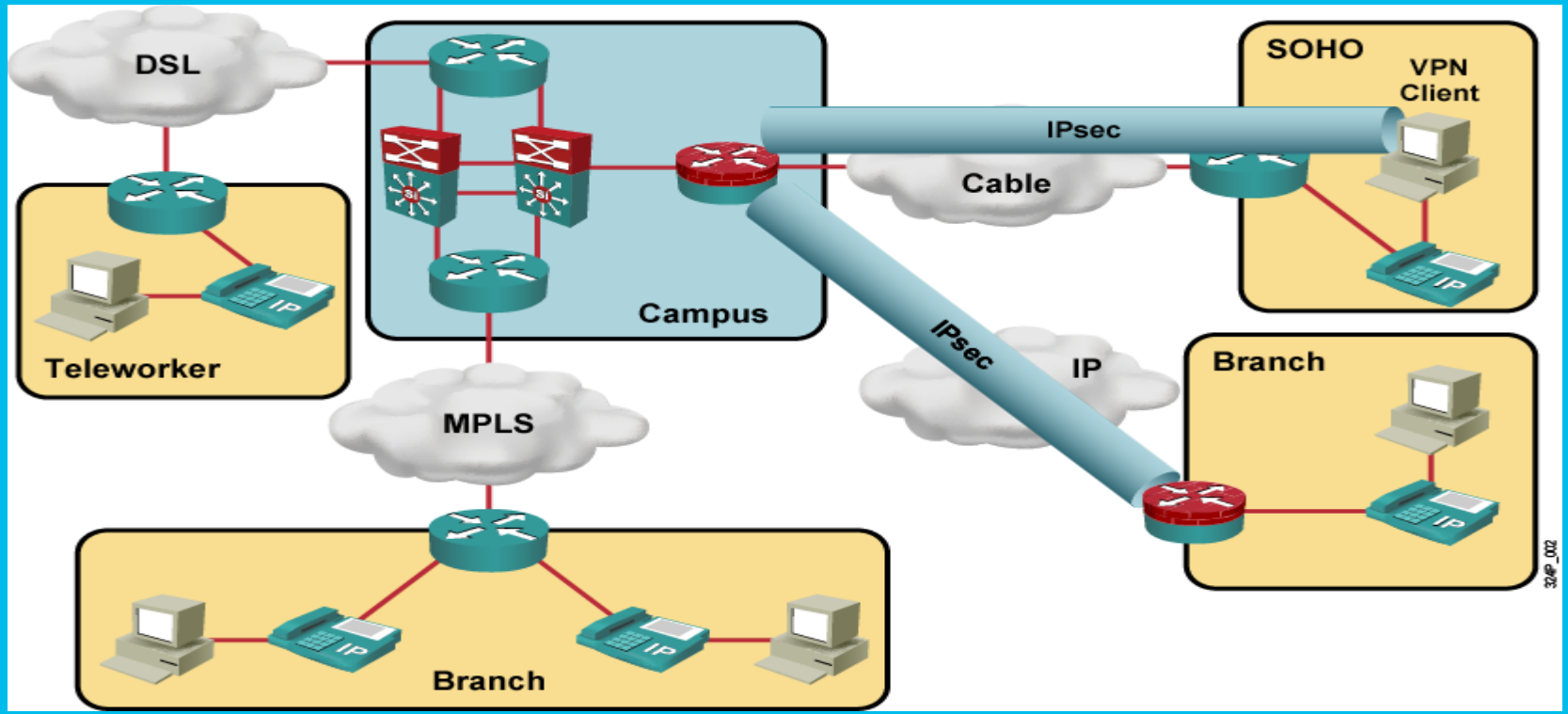
咨询热线：021-61243600

VPN技术的起源

随着互联网技术的发展，网络用户期望在跨越互联网的多个远程结点之间，模拟出专线连接的效果，于是人们在拥有私有IP的数据包外层封装公网IP进行数据传输，使得远程结点之间可以使用私有地址（跨越公网）进行通讯，这种类似于隧道应用的技术，后来被称之为虚拟专用网络（VPN）。

VPN技术的实质是在公共网络上建立企业（或家庭）内部私有的网络，它使得传统网络在连通的灵活性和数据的安全性方面有了显著的提升。而动态多点VPN（DMVPN）是所有现有的VPN连通性技术之中的“集大成”者。

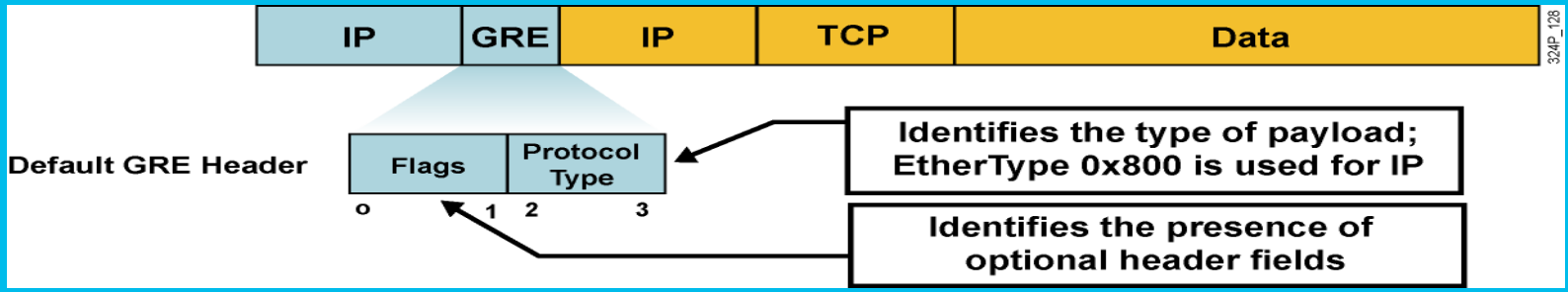
Example: Integrated Services for Secure Remote Access



Generic Routing Encapsulation

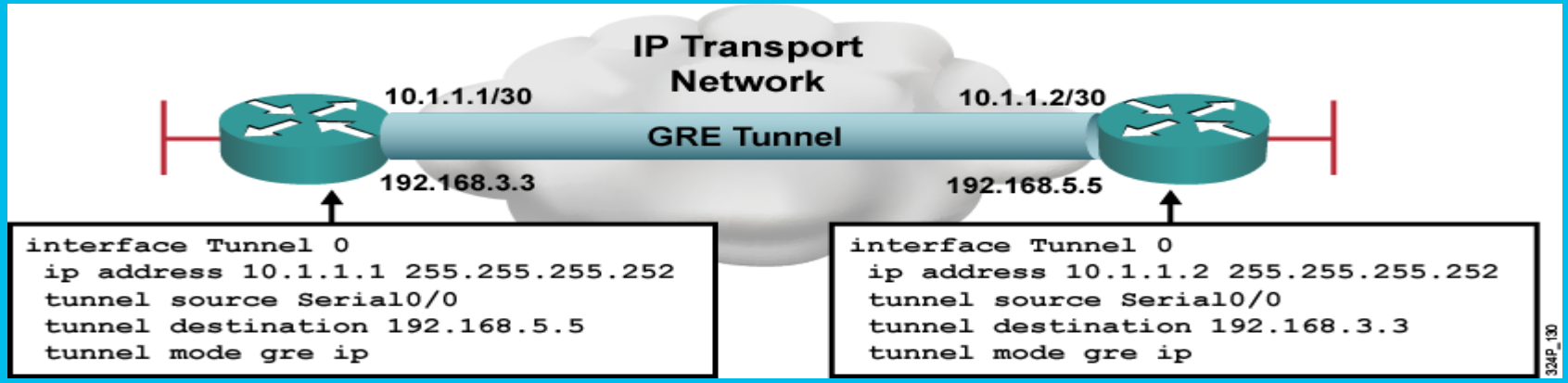
- OSI Layer 3 tunneling protocol:
  - Uses IP for transport
  - Uses an additional header to support any other OSI Layer 3 protocol as payload (e.g., IP, IPX, AppleTalk)

Default GRE Characteristics



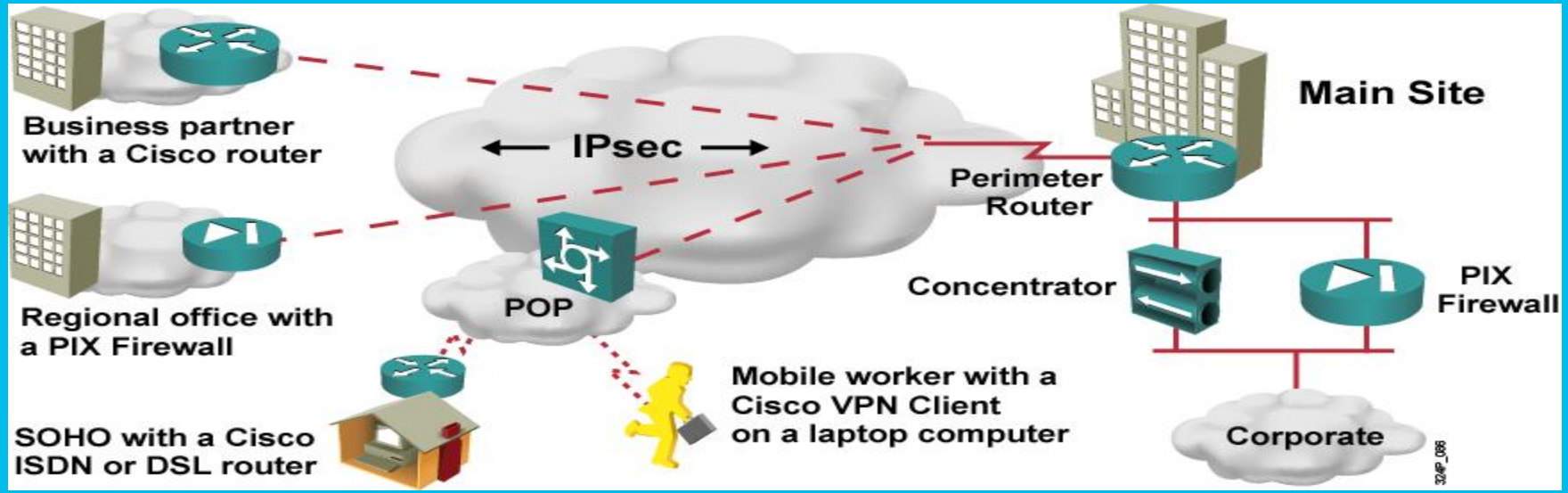
- Tunneling of arbitrary OSI Layer 3 payload is the primary goal of GRE
- Stateless (no flow control mechanisms)
- No security (no confidentiality, data authentication, or integrity assurance)
- 24-byte overhead by default (20-byte IP header and 4-byte GRE header)

GRE Configuration Example



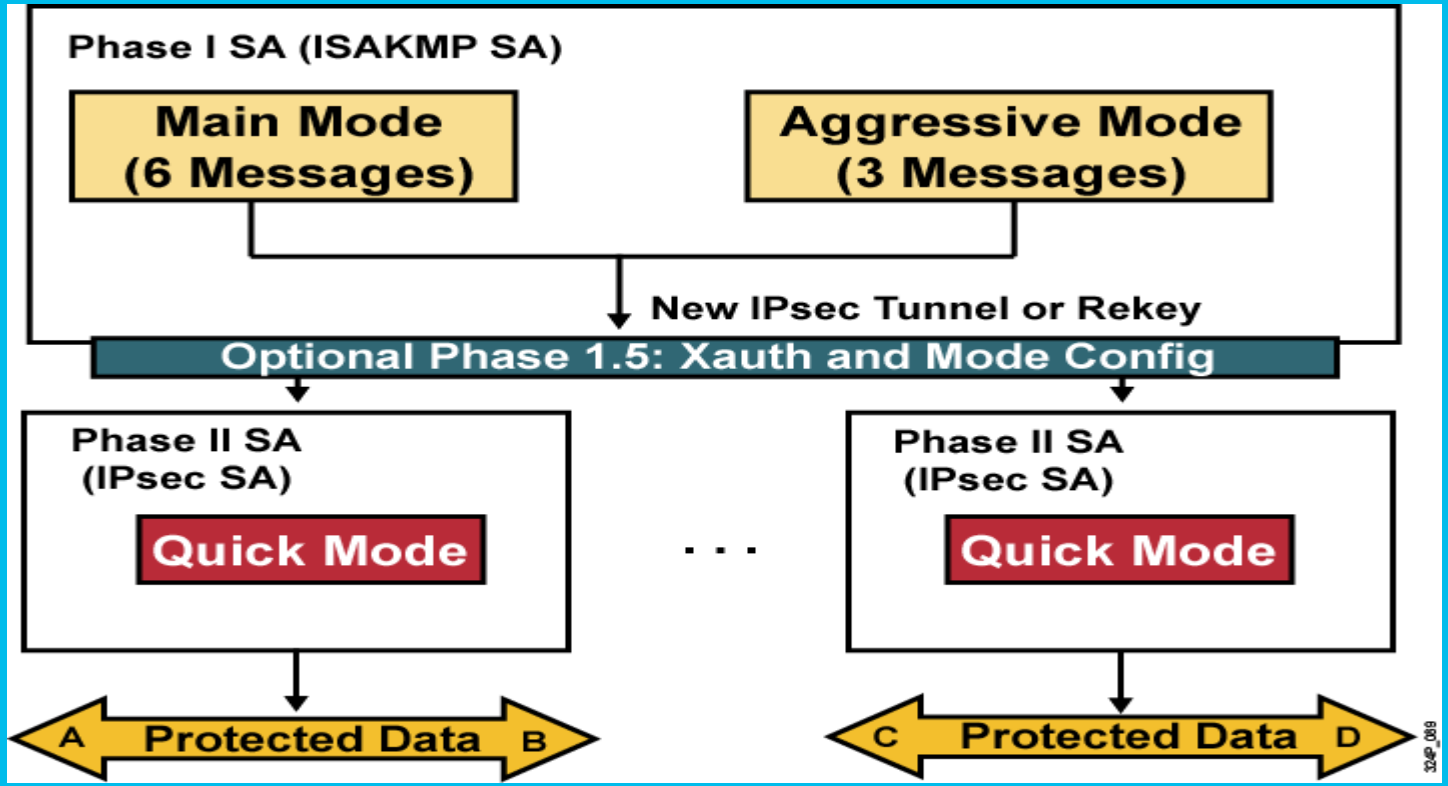
- GRE tunnel is up and protocol up if:
  - Tunnel source and destination are configured
  - Tunnel destination is in routing table
  - GRE keepalives are received (if used)
- GRE is the default tunnel mode.

IPsec Security Features



- IPsec is the only standard Layer 3 technology that provides:
  - Confidentiality
  - Data integrity
  - Authentication
  - Replay detection

IKE Modes

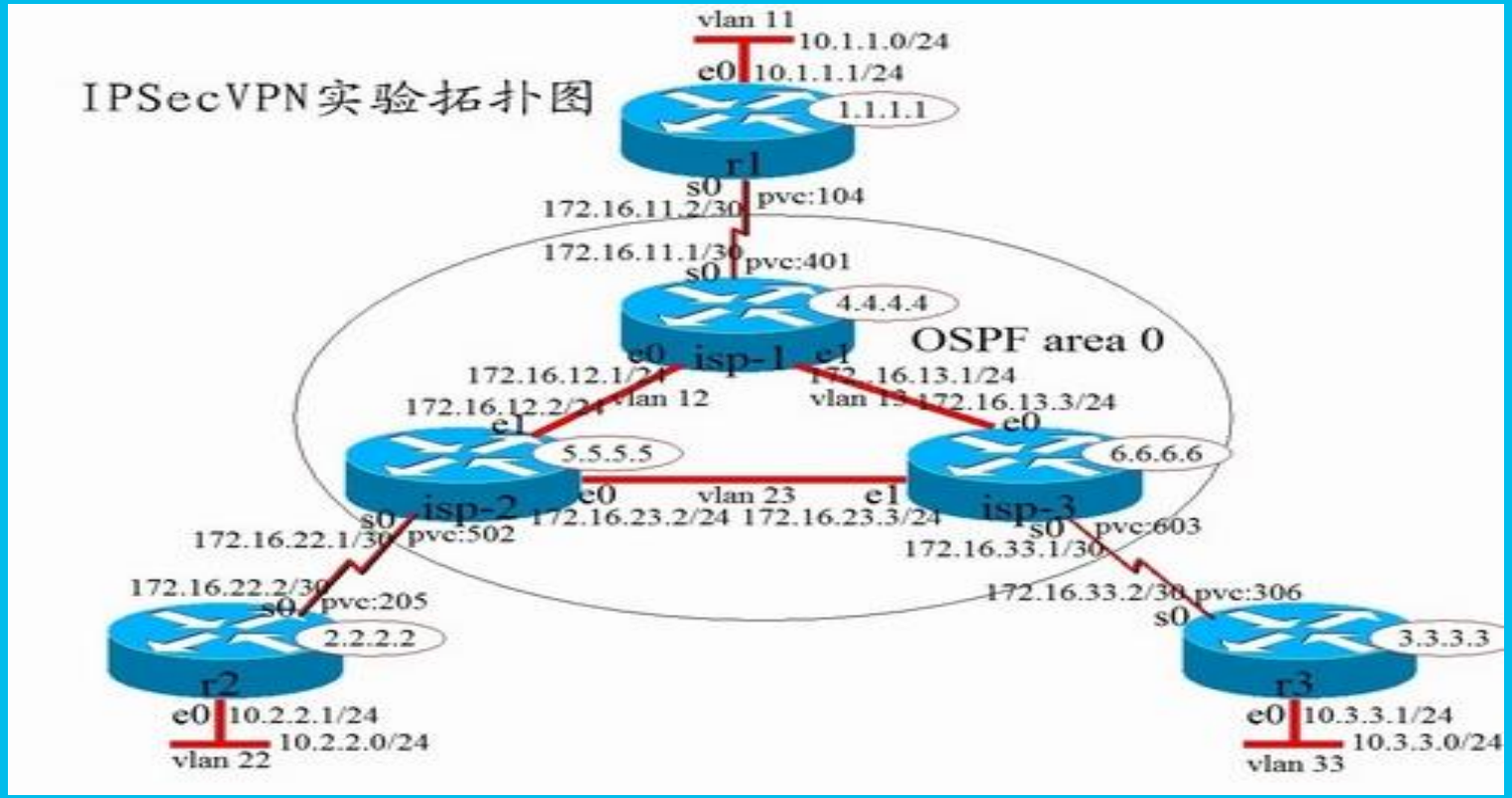

Phase I SA (ISAKMP SA)
Main Mode
(6 Messages)
Aggressive Mode
(3 Messages)
New IPsec Tunnel or Rekey
Optional Phase 1.5: Xauth and Mode Config
Phase II SA
(IPsec SA)
Quick Mode
Phase II SA
(IPsec SA)
Quick Mode
A
Protected Data
B
C
Protected Data
D

传统VPN技术在使用中所面临的问题

- 1. 使用IPSec带来的问题：

为增强VPN传输的安全性，通常在实际应用中对VPN传输的数据进行数据加密。IPSec以它的可靠性、高效性、通用性使其成为VPN数据加密技术的首选协议。然而，IPSec虽然有隧道工作模式，但其建立的隧道没有点对点连接的功能—— 隧道两端的地址是企业网出口的公网地址，在通常情况下，这两个地址不可能在同一个网段，而在两端拥有不同网段IP 地址的路由器之间，是不能建立动态路由协议邻居关系的。—— 没有路由协议的支持，网络的应用规模将大大地受限。

Site-to-Site的IPSecVPN互联环境



传统VPN技术在使用中所面临的问题

- 2. 配置复杂性的问题：

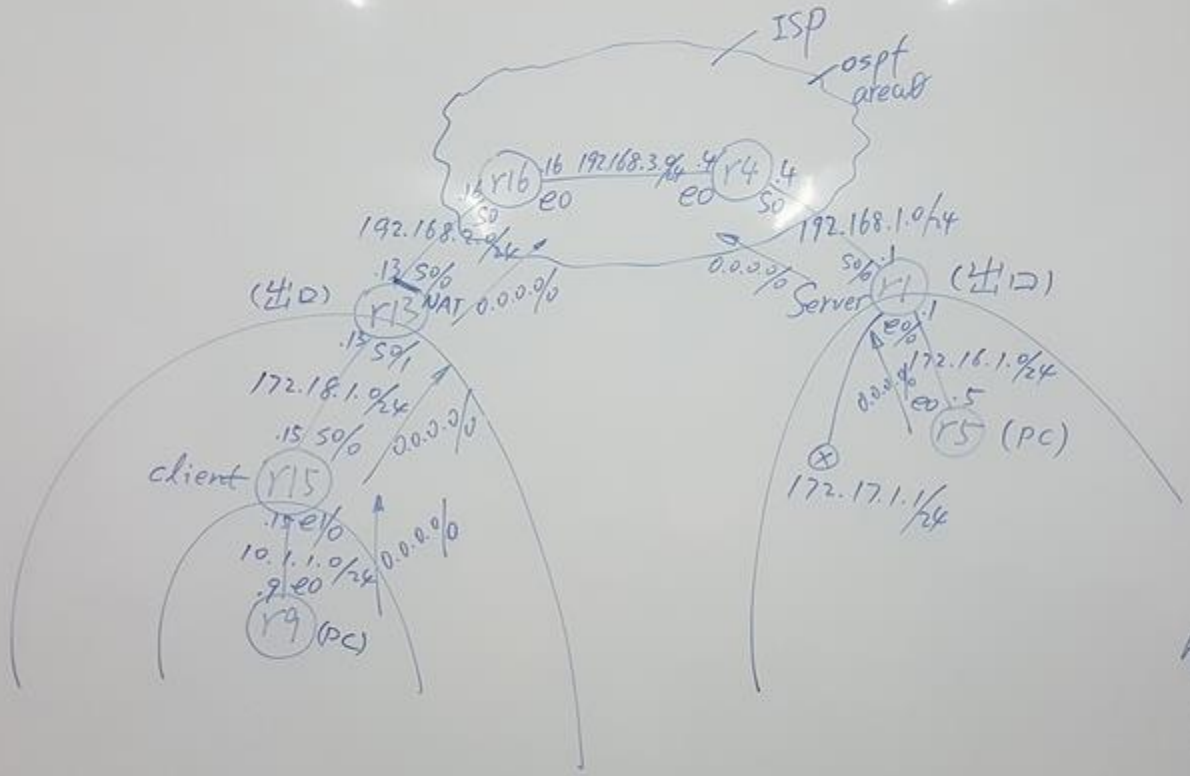
启用IPSec的时候，在众多场合下，引入GRE是必不可少的—— 用GRE实现的VPN可以使远程结点路由器的逻辑接口处于同一个网段，从而使路由协议可以在VPN上得以实施。但是，在（GRE）互联环境下，远程结点之间一对一的GRE隧道（配置）使得在大规模的网络应用中，设备配置变得异常复杂；即使在（GRE）星型联接环境下，核心结点的配置也会随着分支结点的增多而线性地增长，而且分支结点网络之间的通讯数据都必须经过核心结点进行传递，这也使得整个VPN网络的冗余性和数据通讯效率都被大打折扣。

Easy VPN

- Dynamically updated:
  - Central services and security policy
  - Offload VPN function from local devices
  - Client and network extension mode

- Internal IP address
- Internal network mask
- Internal DNS server
- Internal WINS server
- Split tunneling
- IPsec transforms

- Centralized control:
  - Configuration and security policy pushed at the time of the VPN tunnel establishment



假设:

- 192.168.x.x 公网
- 10.x.x.x 内网
- 172.x.x.x 内网

传统VPN技术在使用中所面临的问题

- 3. 被保护网络的连通性问题：

Easy VPN、SSL等VPN接入技术可以做到在客户端结点（分支结点）增加的时候，其服务器端结点（核心结点）配置不增加，对这些技术的采用，可以解决大规模网络应用中的配置复杂性问题，但这时候，藏身各个远程结点之后的被保护网络（内网）的连通性又出现了问题：只有客户端（分支结点）网络可以主动发起到服务器端（核心结点）网络的通讯，而各个结点（被保护）网络之间无法实现对等的通讯。

传统VPN技术在使用中所面临的问题

- 4. VPN结点的固定IP地址问题：

通常情况下，VPN接入结点多采用“宽带接入”的网络接入方式，接入IP地址很难固定，这就为VPN Site-to-Site对等连接环境的应用部署增加了难度。

动态多点VPN“集大成”

- 1. 与GRE技术相结合：

动态多点VPN运用了多点GRE技术，即一个点可以通过一个（多点）GRE隧道同时连接多个点，这就使得某远程结点无论与多少个（其它）结点（逻辑）相连，都只需要建立一个隧道（tunnel）接口。这样做带来的好处是：用GRE实现的VPN，可以运行动态路由协议；在接入结点增加的时候，比如从几个接入结点翻增至上千个接入结点，其核心结点配置不增加，也无须做任何配置修改。由于路由协议的运用，实际上可以实现VPN Site-to-Site对等连接环境，使得各结点被保护网络相互之间的访问不再受限。

动态多点VPN“集大成”

- 2. 下一跳解析协议（NHRP）的运用：

NHRP协议解决了VPN连接中只需核心结点IP地址固定，而分支结点地址可随机分配，以及分支结点之间可直接进行通讯的问题。—— 在NHRP运行的环境下，分支结点在启动后，会向核心结点通告自己的物理接口公网IP地址，有了分支结点的IP地址，核心结点就可以顺利地与分支结点建立VPN隧道（tunnel）实现连通；而当某分支结点要与其它分支结点进行通讯的时候，可以向核心结点索要其它结点的物理接口公网IP地址，之后自行（且自动地）与其建立VPN隧道实现连通，即分支结点被保护网络（内网）之间可不通过核心结点而直接进行数据通讯。

应用配置实例

- 假设有1、2、3三个结点，其中1为核心结点，2、3为分支结点，三者之间建立动态多点VPN，实现（穿越公网的）三个结点之间的VPN通讯，其中，只有结点1的公网接口地址固定为：203.1.1.1，（规划）隧道地址分别为：192.168.1.1，192.168.1.2、192.168.1.3。

应用配置实例

- 核心结点1的配置为：

```
int tunnel 1
 ip address 192.168.1.1 255.255.255.0
 ip nhrp network-id 1
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 tunnel source Serial0/0
 tunnel mode gre multipoint
```

应用配置实例

- 分支结点2的配置为：

```
int tunnel 1
 ip address 192.168.1.2 255.255.255.0
 ip nhrp network-id 1
 ip nhrp authentication cisco
 ip nhrp nhs 192.168.1.1
 ip nhrp map 192.168.1.1 203.1.1.1
 ip nhrp map multicast 203.1.1.1
 tunnel source Serial0/0
 tunnel mode gre multipoint
```

应用配置实例

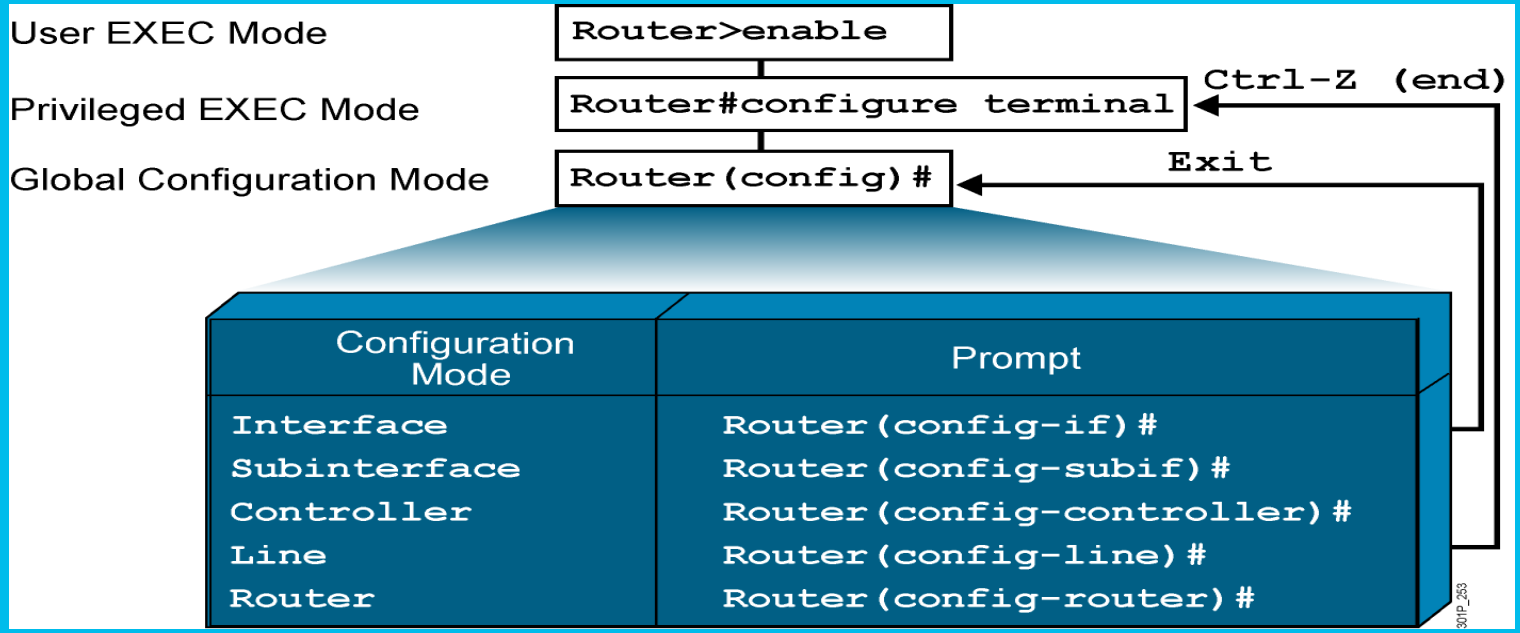
- 分支结点3的配置为：

```
int tunnel 1
 ip address 192.168.1.3 255.255.255.0
 ip nhrp network-id 1
 ip nhrp authentication cisco
 ip nhrp nhs 192.168.1.1
 ip nhrp map 192.168.1.1 203.1.1.1
 ip nhrp map multicast 203.1.1.1
 tunnel source Serial0/0
 tunnel mode gre multipoint
```

应用配置实例

- 核验命令为：在核心结点上show ip nhrp brief，查看是否有分支结点传上来的登记信息。
- 如果希望引入IPSec加密，可以在各设备tunnel接口上配置"接口保护"命令：tunnel protection ipsec profile DMVPNPROFILE，其中DMVPNPROFILE为预先定义的IPSec profile。

Overview of Router Modes



Questions?

问卷调查_思科社区公开课

为帮助我们把CSC公开课活动越做越好，请您拿出一分钟时间，完成问卷调查。

链接：https://www.ciscofeedback.vovici.com/se/6A5348A73BB32C11

完整填写问卷的用户有机会获得社区赠送的精美礼品。

感谢您的参与。获奖信息公告，稍后会在思科服务支持社区发布。

资料分享_思科社区公开课

本次讲座的文档资料和演讲视频稍后也会在社区发布。

会后徐老师会继续做客社区【专家面对面】 活动，对于今天的主题仍有问题，可以在活动专题贴下提出，链接：

http://bbs.csc-china.com.cn/forum.php?mod=viewthread&tid=988759

请继续关注 思科社区，我们会定期为大家带来更多精彩讲座和活动。


CISCO