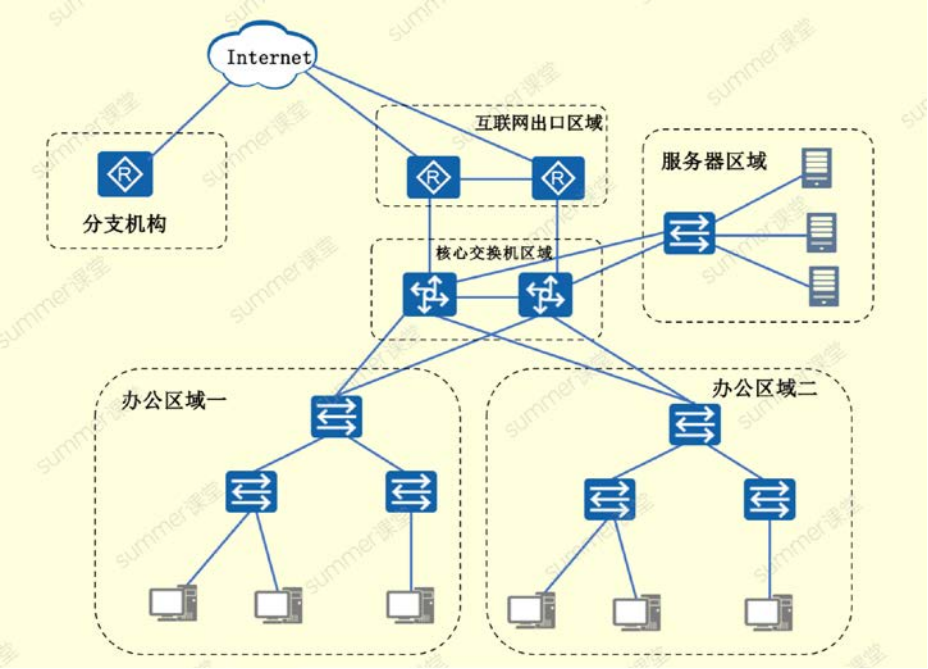
试题一（25分）

阅读以下说明，回答问题1至问题3，将解答填入答题纸对应的解答栏内。

【说明】某企业网络拓扑如图1-1所示。



【问题1】（16分）

请按照网络安全等级保护第三级要求，为该企业规划安全区域边界层面的网络安全防范方案、简要说明方案中网络安全设备的部署规划（包括设备名称、部署区域、部署方式），并说明每个设备在网络安全防范体系中的作用。

【问题2 】（6分）

在网络边界部署防火墙时，防火墙会默认划分Local、（1）、Untrust、DMZ四个安全区域，根据业务需要，管理员新建了一个名为Server的安全区域，优先级为90，这五个安全区域按照优先级从高到低的排序为（2）>（3）>（4）>（5）>（6）。

【问题3】（3分）

以下为防火墙策略配置代码。

[FW] policy interzone trust untrust inbound

[FW-policy-interzone-trust-untrust-inbound] policy 1

[FW-policy-interzone-trust-untrust-inbound-1] policy service

service-set https

[FW-policy-interzone-trust-untrust-inbound-1] action permit

[FW-policy-interzone-trust-untrust-inbound-1] policy 2

[FW-policy-interone-tust-untrust-inboud-2] policy service

service-set icmp

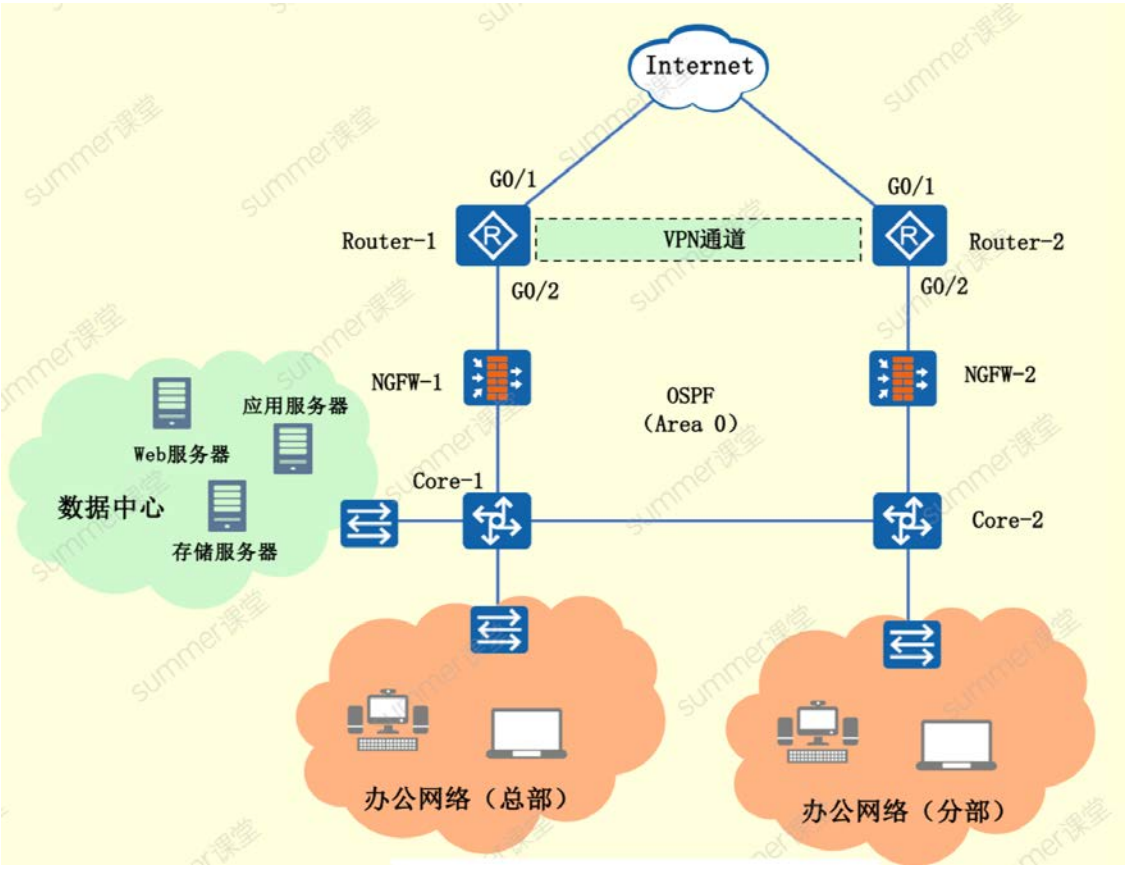
[FW-policy-interone-tust-untrust-inbound-2]action deny

请简要说明上述策略配置代码的作用。

试题二（25分）

阅读以下说明，回答问题1至问题4，将解答填入答题纸对应的解答栏内。

【说明】某企业拓扑如图2-1所示，已知总部Core-1与分布Core-2之间租用专线链路互联，作为两个单位主通信线路，总部的Router1与分部的Router2通过Internet线路构建VPN通道，最为两个单位的备用线路。总部的Router-1、Core-1和分部的Router-2、Core-2之间运行OSPF，配置为单区域Area 0。NGFW-1、NGFW-2以透明模式（业务接口工作在二层）部署在网络中。



【问题1】（10分）

该企业规划的VPN通道起点和终点分别为总部Router-1、分部Router-2的Internet接口，通过VPN通道传输的数据应进行加密保护，同时尽可能提升总部与分支之间VPN通道传输的效率。网络管理员老夏经过需求分析，可选的VPN技术有GRE VPN技术和IPSec VPN技术，结合题目请回答以下问题：

1.老夏进行了GRE与IPSec的优劣势分析，发现二者优缺点互补，将二者同时启用才能满足业务需求，请问将二者同时启用的VPN技术是（1）。

2.老夏规划IPSec的封装模式选择（2），对传输的IP报文进行保护的安全协议选择（3）。

3.在此场景下，IPSec通过ACL定义需要保护的数据流，参照以下地址规划表，则总部Router-1上配置ACL匹配的源地址为（4），目的地址（5）。

区域	设备	接口	网络地址	业务说明
总部	Router-1	G0/1	123.63.146.7/28	Internet出口
		Tunnel0	10.10.0.1/24	GRE隧道地址
	Core-1	Vlanif100	10.10.1.1/24	数据中心业务
		Vlanif200	10.10.2.1/24	办公区有线用户
分部	Router-2	G0/1	210.5.75.3/27	Internet出口
		Tunnel0	10.10.0.2/24	GRE隧道地址
	Core-2	Vlanif100	10.20.2.1/24	办公区有线用户

【问题2】（8分）

在网络中配置OSPF时，网络管理员进行了优化操作，请回答以下问题：

1.为提高链路状态变化时OSPF的收敛速度，可在Router-1、Router-2、Core-1、Core-2上配置（6）与OSPF联动，可以快速检测链路状态，使得故障检测时间可以达到毫秒级。

2.管理员规划在Router-1、Router-2上为OSPF引入缺省路由，由OSPF将缺省路由通告全网。在Router-1、Router-2采用手动配置命令方式，配置完成后路由器将产生一个（7）LSA，并通告到全网，达到全网缺省路由学习的目的。

3.为提高OSPF的安全性，当用户接口启用OSPF时，可在用户接口上配置（8），防止非法设备接入用户网络与现网设备建立邻居关系，这也是防止路由环路的一种方法；同时启用OSPF的（9）认证，对本区域所有接口下的OSPF报文进行认证，防止非法设备与网络设备建立邻居关系。

【问题3】（4分）

该企业计划对总部数据中心的Web业务进行IPv6改造升级。网络管理员对现网评估后规划在Router-1配置NAT64方式实现，通常该方式需要搭配（10）以起实现。已知NAT64前缀为：2001:CD:5:10A::/64，WEB服务器IPv4地址为：124.75.36.100，请问IPv6用户最终向该WEB服务器发起访问的IPv6地址为（11）。

【问题4】（3分）

为保证企业内网安全，该企业计划启用网络准入认证方案，对所有接入网络的设备进行统一的认证和访问授权管理。已知现网设备支持的认证方式有PPPoE、802.1x、MAC认证和Web认证。请针对以下场景选择合适的认证方式，同时保证不为业务带来额外的开销。

1.企业内生产部门、研发部门等人员集中、信息安全要求严格的区域，设备接入网络需进行（12）认证。

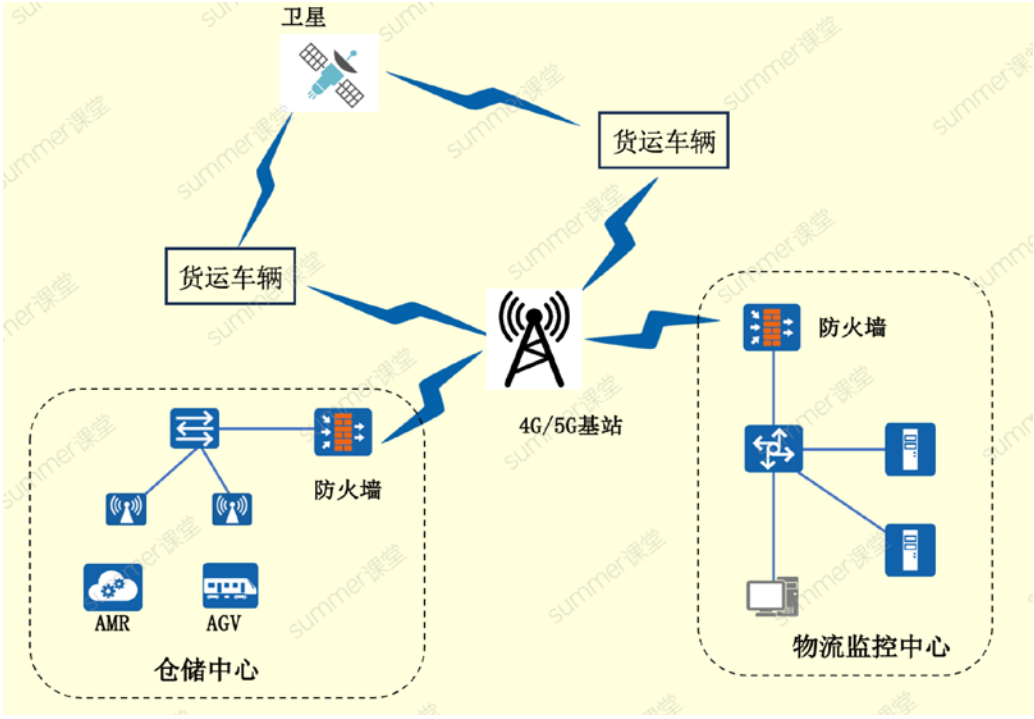
2.针对企业会客厅、接待室、访客室等访客、临时人员可能停留的区域，开通访客网络进行（13）认证。

3.企业中还存在打印机、传真机、智能门锁等设备，此类设备入网可采用（14）认证。

试题三（25分）

阅读以下说明，回答问题1至问题3，将解答填入答题纸对应的解答栏内。

【说明】某物流企业网络如图3-1所示。物流监控中心负责货运调度。货运车辆通过接收GPS信息，将车辆信息及其状况发回物流监控中心。仓储中心的AGV（Automated Guided Vehicle）、AMR（Automated Mobile Robot）等通过Wi-Fi接收指令进行自动化运行。



【问题1】（10分）

请从实际运营的角度，对图3-1所示的物流企业网络需要配置的软件（平台）、硬件设备进行规划，列出主要软件或平台、硬件名称及实现功能。

【问题2】（10分）

AGV使用的无线Wi-Fi网络规划设计有哪些要求?

【问题3】（5分）

简要说明5G在提升物流网络效能方面发挥的作用。

答案解析:

第一大题:

【问题1】（16分）

请按照网络安全等级保护第三级要求，为该企业规划安全区域边界层面的网络安全防范方案、简要说明方案中网络安全设备的部署规划（包括设备名称、部署区域、部署方式），并说明每个设备在网络安全防范体系中的作用。

答案:

（1）在互联网出口/分支机构区域部署防火墙，串行部署，进行网络边界隔离。

（2）在服务器区域部署防火墙或WAF，串行部署，进行区域边界隔离，防止未授权的访问。

（3）在核心交换机区域部署防火墙板卡，与核心交换机集成部署，进行办公区域隔离。

（4）在办公区域部署防火墙，串行部署，对进出办公区域的流量进行检测。

（5）在互联网出口区域部署IPS，串行部署，对进出网络的流量进行安全检测。

（6）在核心交换区域部署IDS，旁路部署，对重点流量进行镜像检测分析。

（7）在互联网出口部署沙箱，旁路部署，对异常流量进行深入检测和分析。

（8）在互联网出口部署上网行为管理，串行部署，对用户访问互联网的异常行为进行阻断和记录。

（9）在互联网出口区域部署防毒墙、防垃圾邮件系统，串行部署，对病毒和垃圾邮件进行过滤。

（10）在互联网出口区域和核心交换区域部署日志审计系统，旁路部署，对进行网络和跨区域的流量和日志进行审计记录。

（11）在服务器区域部署堡垒机，旁路部署，对运维进行审计记录。

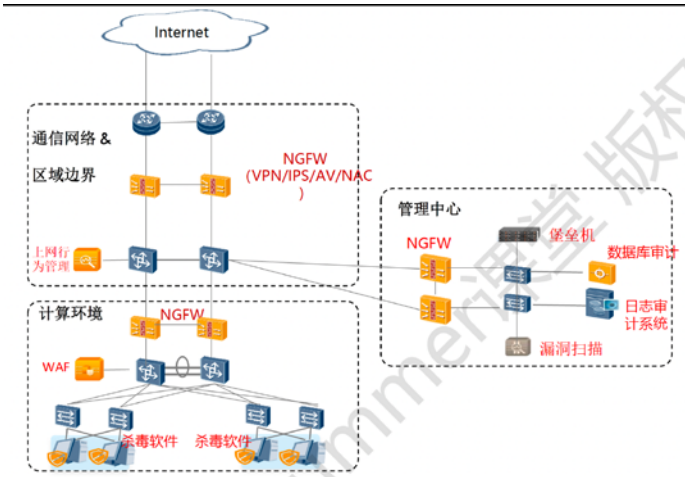
（12）基于可信根对区域边界设备的系统引导，应用关键点可动态验证可报警、可审计。

注：至少写8点，尽量多写，多写不扣分。

解析：关键词“安全区域边界”，这是等保 2.0 的内容。有 2 种逻辑，以安全设备为核心去说，或者以区域为重点展开。

等保2.0技术要点—等保三级

等保技术要求	子项	主要内容	对应产品
安全通信网络	网络架构 G	选型合理，分区隔离，冗余架构，高峰可用	NGFW、防DDoS
	通信传输 G	采用校验技术/密码技术保证通信过程中数据的完整性和保密性	NGFW（IPSec & SSL VPN）
	可信验证 S	基于可信根对通信设备的系统引导，应用关键点动态验证，可报警、可审计	网络设备可信启动机制
安全区域边界	边界防护 G	跨边界控制，内联设备，外联行为监测，无线网限制	NGFW、网络准入控制
	访问控制 G	五元组过滤、内容过滤、策略优化、基于应用协议和应用内容的访问控制	NGFW、安全控制器
	入侵防范 G	防外部攻击、防内部攻击、防新型未知网络攻击	IPS/IDS、探针、沙箱
	恶意代码防范 G	网络防病毒、垃圾邮件过滤	NGFW（AV）、NGFW（防垃圾邮件）
	安全审计 G	用户行为、安全事件审计，远程用户行为，访问互联网用户行为单独审计和数据分析	堡垒机，上网行为管理、综合日志审计系统
	可信验证 S	基于可信根对区域设备的系统引导，应用关键点可动态验证，可报警、可审计	设备自身可信启动机制



测评80+分套餐

整体方案说明

【接入边界NGFW】【必配】：融合防火墙安全策略、访问控制功能。解决安全区域边界要求，并开启AV模块功能；配置网络接入控制功能（802.1X）；配置SSL VPN功能；

【分区边界NGFW 】【必配】：用于解决安全分区边界的访问控制问题

【主机杀毒软件】【必配】：解决安全计算环境要求

【日志审计系统】【必配】：解决安全管理中心要求

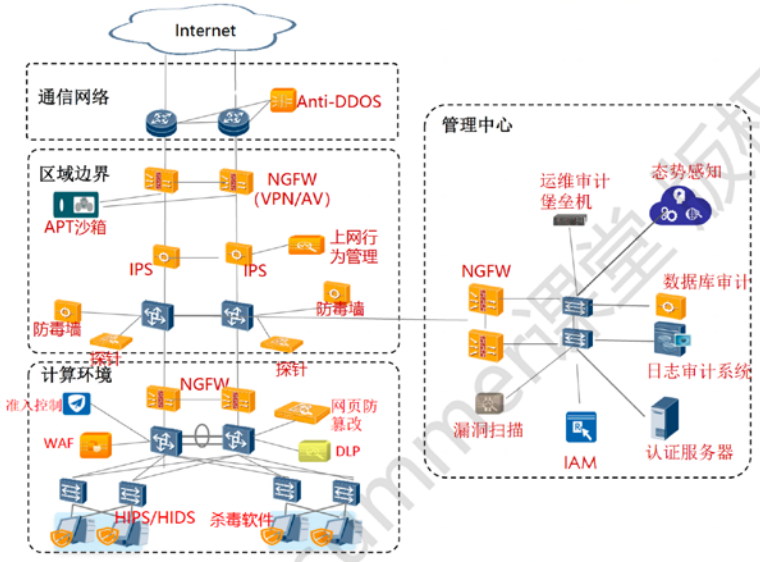
【堡垒机】【必配】：解决集中管控、安全审计要求

【数据库审计】【必选】：解决数据库操作行为和内容等进行细粒度的审计和管理，需要根据系统内是否包含数据库业务系统选择

【漏洞扫描】【必配】；

【上网行为管理】【必选】；

【WAF】【选配】；



测评85+分套餐

整体方案说明

【NGFW】（必选）；开启VPN，AV特性

【IPS】（必选）；解决区域边界入侵防御

【Anti-DDoS】【必选】；

【APT沙箱】【必选】：新型网络攻击行为

【上网行为管理】【必选】；

【日志审计系统】（必选）；

【数据库审计系统】（必选）；

【漏洞扫描】（必选）；

【主机杀毒软件】（必选）；

【态势感知】【必选】；

【WAF应用防火墙】【必选】；

【运维堡垒机】【必选】；

【网络准入控制系统】【必选】；

【认证服务器】【必选】；

【网页防篡改】【可选】；

【主机入侵防御HIPS】【可选】；

【DLP数据防泄漏】【可选】；

【IAM身份鉴别平台】【可选】；

【态势感知探针】【可选】：可复用NGFW的能力

【问题2 】（6分）

在网络边界部署防火墙时，防火墙会默认划分Local、（1）、Untrust、DMZ四个安全区域，根据业务需要，管理员新建了一个名为Server的安全区域，优先级为90，这五个安全区域按照优先级从高到低的排序为（2）>（3）>（4）>（5）>（6）。

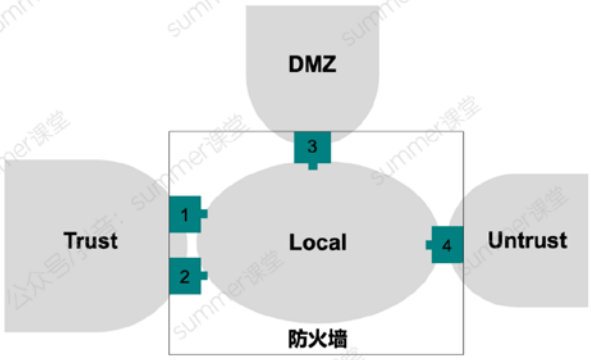
参考答案：

（1）Trust （2）Local （3）Server （4）Trust （5）DMZ （6）Untrust

解析：

防火墙区域划分

- 根据网络的安全信任程度和需要保护的对象，人为划分若干安全区域，包括：



安全区域	安全级别	说明
Local	100	设备本身，包括设备的各接口本身。
Trust	85	通常用于定义内网终端用户所在区域。
DMZ	50	通常用于定义内网服务器所在区域。
Untrust	5	通常用于定义Internet等不安全的网络。

- 受信任程度：Local > Trust > DMZ > Untrust
- Outbound：高优先级 → 低优先级
- Inbound：低优先级 → 高优先级

【问题3】（3分）

以下为防火墙策略配置代码。

[FW] policy interzone trust untrust inbound

[FW-policy-interzone-trust-untrust-inbound] policy 1

[FW-policy-interzone-trust-untrust-inbound-1] policy service service-set https

[FW-policy-interzone-trust-untrust-inbound-1] action permit

[FW-policy-interzone-trust-untrust-inbound-1] policy 2

[FW-policy-interone-tust-untrust-inboud-2] policy service service-set icmp

[FW-policy-interone-tust-untrust-inbound-2]action deny

请简要说明上述策略配置代码的作用。

参考答案：

配置安全策略，放行untrust到trust的https流量，拒绝icmp流量。

解析：

要知道什么是防火墙的inbound，即从低安全区域，访问高安全需要。

第二大题：

问题 1：

参考答案：

（1）GRE over IPSec （2）传输模式 （3）ESP

（4）123.63.146.7/28 （5）210.5.75.3/27

解析：

GRE支持组播，明文传输，IPSec支持加密，但不支持组播，而题目需要跑OSPF，会有组播流量，所以需要将GRE和IPSec结合，即GRE over IPSec，一般很少用IPSec over GRE，这样也不能支持组播，因为IPSec已经加密了，GRE看不到里面的内容。

传输模式和隧道模式的区别如下：

（1）安全性不同：隧道模式下可以隐藏原始报文的IP地址、协议类型和端口，从而完整地对原始报文进行加密和验证。

（2）对性能的影响不同：隧道模式下生成了一个额外的IP头，因此会比传输模式占用更多的带宽资源。

（3）应用场景不同：传输模式主要应用于“主机-主机”或“主机-网关”之间的通信；隧道模式主要应用于“网关-网关”或“主机-网关”之间的通信。由于GRE封装时已经增加了一个公网IP头，而隧道模式跟传输模式相比又增加了一个新的公网IP头，从而使报文长度更长，效率低，题目要求尽可能提升传输效率，所以要采用传输模式。

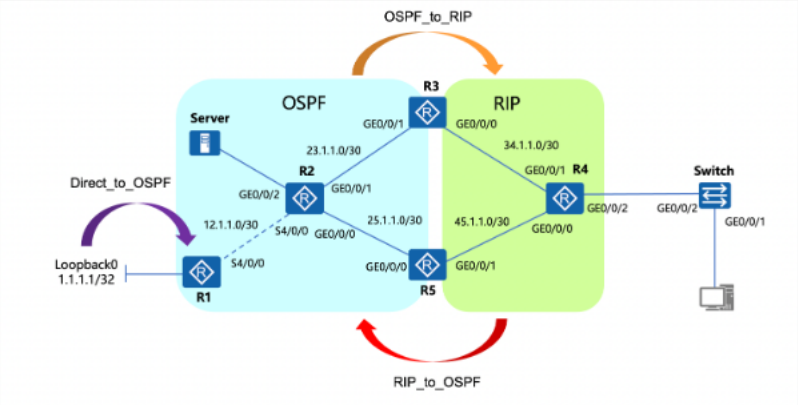
第二大题，问题 2

（6）BFD （7）5类 （8）静默接口 （9）区域

解析：

GRE支持组播，明文传输，IPSec支持加密，但不支持组播，而题目需要跑OSPF，会有组播流量，所以需要将GRE和IPSec结合，即GRE over IPSec，一般很少用IPSec over GRE，这样也不能支持组播，因为IPSec已经加密了，GRE看不到里面的内容。

静默接口，考试前网工的冲刺题，网规SVIP都做过，路由器连用户设置为静默接口，交换机连用户设置为边缘接口。下面这个题还有印象吗？



【2023年11月网工考前冲刺题-案例分析三/问题3】（4分）
为了加快网络收敛，节省网络资源，可以在R2和Switch哪些接口上进行什么配置？（4分）
【参考答案】
（1）将R2连接服务器的接口配置为静默接口，不发送Hello报文，降低R2系统和带宽压力，也避免了对Server的性能降低。配置参考如下：
[R2] ospf 1
[R2-ospf-1] silent-interface GigabitEther0/0/2

（2）将Switch连接PC的接口设置为边缘端口，无需经历 STP 计算，快速进入转发状态，主要针对于接服务器或主机的交换机端口。配置参考如下：
[Switch]interface GigabitEthernet0/0/1
[Switch-GigabitEthernet0/0/1]stp edged-port enable
【这不就是考的原题吗？】

第二大题，问题 3：

参考答案：

（10）DNS64 （11）2001:CD:5:10A::7C4B:2464

解析：

124.75.36.100转换为十六进制是7C.4B.24.64，故变换后的IPv6地址是2001:CD:5:10A::7C4B:2464。

参考答案：

（12）802.1x （13）Web （14）MAC

解析：

各种认证的特点和应用场景，必须掌握。

第二大题，问题 4：

第三大题，问题 1：

（2）车辆运行状态采集设备（含GPS模组），采集车辆的运行时速、位置、驾驶员状态等信息。

二、传输层

（1）Wi-Fi系统：包括AP、AC和PoE交换机等设备，为仓储中心智能设备提供无线接入服务。

（2）GPS模组：通过卫星传送位置信息（购买服务即可）。

（3）4G/5G网络：配置4G/5G流量卡，通过运营商网络传输车辆状态信息。

三、应用层

（1）硬件：服务器、存储、交换机、防火墙、管理PC等硬件设备。

（2）软件平台（本次网工考试里面有提醒）

① 仓储管理平台：对货物出入口、堆存、保管、保养、维护等进行管理。

② 物流监控平台：权衡运输服务和运输成本，对运费，运输时间，频度，运输能力，货物的安全性，时间的准确性，适用性，伸缩性等综合分析和评估，并进行货运调度（题干已知的写上去）。

③ PLC控制服务器：安装工控平台，实现前端AMR和AGV的智能控制。

④ 运维审计平台：对用户登录和权限进行统一管理，并审计用户操作。

第三大题，问题 2：

参考答案：

（1）无盲区：AGV运行区间Wi-Fi信号全覆盖，无信号盲区。（一般通过调整AP功率实现）
（2）信号好：AGV运行线路的无线覆盖强度需要≥-75dbm，S/N（信噪比）≥30dbm。（一般通过调整AP功率实现）
（3）干扰低：信道应与其他网络信号信道交错，避免同频干扰。同时调整AP功率，控制合适的重叠区域，不宜过大也不宜过小。
（4）屏蔽和干扰：所有无线接入点（AP）需要保证无线信号强度符合要求的同时，也必须将AP安装在无遮挡的位置，以便AP与AGV通讯不受金属障碍物影响。避免微波炉、电气化铁路等干扰源。
（5）漫游：配置无线控制，统一管理所有AP，实现AGV等设备无线漫游。
（6）需要提供一个覆盖全场的独立专用网络或单独的SSID，该SSID需要在同一IP网段内，最好是能划分专用VLAN。中央控制主机需要提供网线接入，中控主机所在网段与AGV专用SSID同属一个网段，所划分的AGV专用VLAN或共享网段请与办公网/业务网隔离，且不要在该段中配置各种访问策略/上网认证，避免阻断AGV通讯包和端口通讯。
（7）无线接入点（AP）设备必须支持至少30个用户数的接入，避免因AP接入负荷大而导致AGV等设备无法正常接入。
（8）通讯响应时间平均20m/s。
（9）测试AGV接入无线网运行持续4小时的ping包情况，需要保证在1000字节/pkg的连续ping包下，丢包率必须≤1%。ping包过程不能出现超过2个的连续丢包。
（10）无线接入点（AP）支持802.11ac/b/g/n/ac/ax协议，开启Wi-Fi2.4G/5.8G网络。

解析：

开放性题，合理即可，可写内容非常多。

第三大题，问题 3：

参考答案：

（1）降低运输成本。通过获取前端道路信息，综合并通过5G下发最优线路，节省成本。
（2）提供物流效率。5G技术具有高速度和低时延的特点，这使得智慧物流的数据传输速度更快，稳定性更高。这为智慧物流中的各种应用场景，如智能配送、智能仓储、智能运输等提供了更精准、更高效的数据支持和服务。
（3）改善服务质量：提供端到端的监控覆盖、物流跟踪以及盗窃防范等功能。
（4）推动物流行业的数字化转型，积累大数据，让物流行业发展有迹可循。

解析：

开放性题，合理即可，可写内容非常多。