WebRAY 盛邦安全 | 股票代码 688651

让网络空间更有序

卫星互联网安全年度报告

2024

联合发布单位：

南京航空航天大学

远江盛邦安全科技集团股份有限公司

南京天际易达通信技术有限公司

版权声明

报告撰写单位及撰写人：

南京航空航天大学

李广侠、程剑、吕晶

远江盛邦安全科技集团股份有限公司

权晓文、郑重、何鹏程、郝龙

南京天际易达通信技术有限公司

李辉、程伟、梁凝睿

前 言

卫星互联网是对传统卫星通信网络的深度重构，它以互联网为底座，融合地面移动网络，通过星间链路和地面信关站形成空天地一体化的互联架构，提供全球范围的互联网接入服务。从本质上看，卫星互联网是一个广域接入服务网络，而传统卫星通信网主要解决地面网络覆盖不到地区的通信需求，二者在功能和应用上存在显著差异。

凭借随时随地接入互联网的特性，卫星互联网在军事、航空、海事等领域展现出巨大潜力，并被视为未来6G网络的重要雏形。它不仅推动了经济增长，也成为国家信息基础设施建设和全球信息竞争的战略高地。然而，随着卫星互联网的加速发展，其面临的网络安全挑战也日益凸显，全球范围内的卫星网络攻击事件呈现高频化、攻击面扩大化的趋势。

卫星互联网依赖于先进的信息技术和复杂的系统集成，其开放的网络架构和高度互联的特性，使其面临前所未有的网络安全风险。一方面，网络攻击手段日趋多样，卫星通信的安全防护难度加大；另一方面，卫星通信链路的复杂性增加，用户端流量管控需求愈发强烈，同时，运维管理的安全保障也面临更大挑战。面对这些问题，如何构建高效、可靠的安全防护体系，已成为卫星互联网发展的重要课题。

基于此，本报告梳理了卫星互联网的应用范围，剖析了近期主要的安全事件及其技术原理，梳理、归纳了卫星互联网的安全风险，并提出可行的理论参考与实践建议。

作为新兴领域，卫星互联网的安全需求日益复杂化、多样化，未来还将面临更多挑战。保障卫星互联网安全不仅是技术问题，更关乎责任与信任，需要政府、企业和社会各方的共同努力。只有构建安全、稳定、可靠的卫星互联网生态，才能支撑其长期健康发展。

本报告的撰写，源于我们对行业发展的理解与对网络安全的高度关注。我们诚挚希望本报告能为卫星互联网安全领域的研究者、从业者及关注者提供有价值的启发和参考，共同助力这一领域的长期稳定发展。

目录

Contents

附件 1
针对卫星互联网的观点

附件 2
伊朗油轮事件背后的卫星互联网暗战：iDirect设备测绘与安全风险研究

01

卫星互联网概况

卫星互联网是指通过卫星通信技术实现全球范围内的互联网接入和数据传输的网络系统。它利用在轨卫星作为中继节点，将地面用户终端与互联网骨干网络连接起来，从而实现宽带通信、数据传输、视频流、物联网等多种应用。简单来说：卫星互联网是由分布在不同轨道的空间节点，通过星间链路、星地链路和地面信关站连接在一起，通过融合地面移动网络和互联网，并以互联网为底座，形成空天地一体化组网互联，并提供泛在互联网接入服务的信息基础设施。

卫星互联网是一个泛在互联网接入服务网络，卫星网是采用卫星解决通信、导航及遥感的通信网络，覆盖范围和应用目标是完全不同的，盛邦安全针对卫星互联网的一些观点和看法见附件一。

1.1. 国际互联网发展情况

1) Starlink（星链） [5][6]

截至2025年，“星链”星座在轨卫星规模达8300余颗，在轨服务的有6200余颗，占全球在轨卫星总量超60%。星链在全球运行了150余个信关站，这些信关站主要分布在南北美洲、澳洲及欧洲，用于连接卫星与地面互联网，每个信关站最多可连接8颗Starlink卫星，这些信关站对于星链网络的服务范围和稳定性至关重要。星链终端（Starlink Terminal）的应用场景非常广泛，包括普通用户、房车、企业、海事和航空等。星链已在41个国家落地服务。星链终端在军事领域也有广泛应用，特别是在提高战术火力的精确度和解决作战协调和通信问题上表现出色。全球用户数量突破400万，通常一个用户会对应一个终端，因此可以大致认为星链全球终端数量也在400万台左右。星链网络启用了IPv4和IPv6网络。

2) OneWeb（英国一网） [4]

截至2024年12月，OneWeb星座拥有654颗卫星，信关站数量为44个。这些信关站主要分布在英国、北欧、格陵兰、冰岛、北冰洋、加拿大、非洲、美国主要地区以及中国周边等地。OneWeb支持Ku、Ka频段，虽然OneWeb卫星具备在上行频率12.75–13.25GHz和29.1–29.5GHz频段，下行频率19.3–19.7GHz和19.7–20.2GHz频段内工作的能力，但目前FCC并未批准OneWeb卫星星座使用这些频段。探测到的OneWeb拥有的IPv4地址数量为4,096个，没有启用IPv6网络。

3）Viasat（卫讯）[6]

美国卫讯公司（Viasat）目前拥有并运营19颗在轨卫星，在美国的信关站数量为17个，加拿大的信关站数量为4个。其中服务民航飞机的卫星终端是其特色产品，这些终端设备主要用于支持民航舱内的高速互联网服务，能够在多颗Ka波段卫星之间以及每颗卫星的多点波束之间进行无缝切换，为飞机提供持续不断的空中通信链路。Viasat使用了Ka、Ku、L、S、V频段，其中Viasat通过收购Inmarsat整合Ka、L和S频段的资源，构建了一个全球高容量的空间和地面混合网络，支持多种应用场景，包括宽带互联网接入、机载通信、海事通信和政府通信等。目前启用IPv4和部分IPv6协议，其中可探测的IPv4地址数量约39,424个，Viasat消费者服务不支持IPv6，但是针对政府、军事应用、企业和服务提供商支持IPv6。

4）Hughes（美国休斯）[6]

截至2023年，休斯卫星在轨卫星数量为4颗。这4颗卫星分别是EchoStar-17、EchoStar-19、AMC-15和AMC-16。休斯卫星的服务范围主要集中在美洲地区，通过这些卫星提供的服务包括机载宽带服务。休斯与Thales和SES合作，利用多颗高吞吐量卫星（HTS）的Ka频段资源，共同在美洲和大西洋地区支撑Thales的FlytLive机载宽带服务，能够覆盖整个美洲地区，并对北美地区形成重叠和冗余覆盖，以确保服务的稳定性和可靠性。休斯卫星支持Ka、Ku、C频段。休斯卫星启用了IPv4，尚未全面支持IPv6协议，探测到的休斯卫星网络IPv4地址数量为588,032个。

1.2. 中国卫星互联网发展情况

1）星网

截至2024年12月，星网在轨卫星数量为23颗。根据ITU要求，在2029年底前需发射10%的卫星，即1300颗左右；2032年底前完成至少6,496颗卫星的发射入轨；最迟2035年底前，完成全部12,992颗卫星的发射入轨，星网建设完成并投入使用。

2）千帆

千帆星座计划在2025年底实现648颗卫星提供区域网络覆盖，到2027年底实现全球网络覆盖，2030年底前完成超过1.5万颗卫星的组网。随着卫星组网的推进，与之配套的终端数量也将逐步增加。截至2024年12月23日，千帆星座在轨卫星数量已达到54颗，处于组网的初期阶段，终端数量相对较少，但随着后续卫星的不断发射和组网的完善，预计终端数量会快速增长。

3）中国卫通

中国卫通集团股份有限公司（简称：中国卫通）是中国航天科技集团有限公司从事卫星运营服务业的核心专业子公司，具有国家基础电信业务经营许可证和增值电信业务经营许可证，是我国拥有自主可控通信卫星资源的基础电信运营商，被列为国家一类应急通信专业保障队伍。中国卫通运营管理着19颗优质的在轨民商用通信广播卫星，覆盖中国全境、东南亚、南亚、中东、非洲以及欧洲和太平洋地区。

1.3. 卫星互联网的主要应用

1.3.1. 卫星互联网主要应用领域

卫星互联网主要应用领域包括：

大众应用领域

卫星电话：在地面通信网络覆盖不足的偏远地区、山区、海上等，卫星电话可保障语音通信，如铱星系统的卫星电话。

互联网电视：通过卫星互联网可实现电视节目全球传输与播放，丰富节目内容与传播范围，为偏远地区用户提供更多选择。

卫星宽带：为家庭、企业及公共场所提供高速宽带接入，在无地面宽带网络覆盖区域，用户可借助卫星终端设备接入互联网。

航空航天领域

机载WiFi：为飞机乘客与机组人员提供网络连接，提升飞行体验，如波音787、空客A350等部分机型已配备。

飞行通信与导航：保障飞机与地面控制中心的通信，传输飞行数据、气象信息等，还可通过卫星导航增强系统提高飞行导航精度。

海洋领域

海事卫星电话：为海上船舶提供语音通信服务，确保船舶在远洋航行时的通信联络。

船舶监控与管理：借助卫星通信实时传输船舶位置、速度、航向等信息，实现对船舶的监控与调度，提高航行安全性与运营效率。

交通运输领域

车联网：实现车辆与车辆、车辆与基础设施间的通信，为自动驾驶提供支持，如在无地面网络覆盖的偏远地区保障车辆的安全行驶。

智能交通管理：为交通管理部门提供交通流量监测、路况信息采集等服务，辅助交通决策与管理，优化交通资源配置，提升城市交通运行效率。

物联网领域

物流与资产管理：实现对货物、车辆、设备等的实时定位与状态监测，优化物流配送路线，提高资产管理效率。

环境监测与资源管理：采集环境数据、自然资源信息等，为环境保护、资源开发与管理提供决策依据，如监测森林火情、海洋生态等。

应急救援领域

应急呼叫：在自然灾害等紧急情况下，为受灾地区提供应急通信手段，保障救援人员与受灾群众的通信联络。

数据保护与恢复：对重要数据进行备份与传输，确保数据安全，为灾后重建提供数据支持。

军事国防领域

军事通信：构建军事通信网络，保障军队作战指挥、情报传输等通信需求，确保军事行动的高效指挥与协同。

军事侦察与监视：搭载侦察设备，获取军事目标图像、情报等信息，为军事决策提供支持。

1.3.2. 卫星互联网在低空经济的应用

国家部委及各地方政府纷纷积极出台推动低空经济发展的相关政策。在低空经济的诸多关键要素中，通信基础设施建设占据着核心地位。其建设需要综合考虑网络覆盖范围、性能表现、容灾能力以及应对低空突发事件等多重复杂因素。

目前，无人飞行器的飞行垂直高度为距离地面1000米以下的空间（最高3000米以内），通信传输要求存在显著差异，从10kbps到几百Mbps不等；传输延迟也存在较大波动，介于1ms到100ms之间，通信网络还需实现全域覆盖，飞行控制通信信道需要满足低延迟、高稳定性要求。针对复杂多变的低空场景，5G地面网络不能完全满足低空通信的要求，只能够覆盖250米以下的区域，而从250米到3000米的空域则需要借助卫星互联网来实现可靠的通信保障。

1.3.2.1. 控制链路保障

在超视距飞行时，卫星互联网能突破传统通信距离限制，确保无人机与地面控制站间稳定通信，如“星链”系统可让无人机在全球范围接收指令。

为无人机集群作战提供可靠通信支持，实现多架无人机协同作业，如在军事侦察、搜索救援等场景中，保障无人机间数据共享与指令传输。

1.3.2.2. 数据传输支持

支持无人机实时传输高清视频、图像等大量数据，使地面控制站及时准确掌握现场情况，如卫星通信的宽频带特性可满足无人机在环境监测、测绘等任务中的数据传输需求。对于长航时无人机，卫星互联网能持续稳定传输飞行状态、传感器数据等，确保飞行安全与任务执行效率。

1.3.2.3. 导航定位增强

北斗卫星导航系统等卫星互联网资源可提高无人机定位精度与可靠性，实现精准导航与定位，保障无人机在复杂环境下按预定航线飞行，在农业植保、物流配送等领域发挥重要作用。

1.3.2.4. 拓展飞行范围

使无人机在无地面网络覆盖的偏远地区、海上等执行任务成为可能，如在海洋监测中，无人机可借助卫星互联网将采集的数据实时传输回地面站。支持无人机在军事领域的远程作战与侦察，扩大作战半径与侦察范围，如乌克兰将星链技术应用于无人机，提升了其作战效能。

1.3.2.5. 提升飞行安全性

卫星链路覆盖范围大、电波传播稳定，不受自然环境和人为因素影响，为无人机在恶劣环境下飞行提供稳定通信保障，降低通信中断风险。可实现对无人机的远程监控与管理，及时发现并处理故障隐患，提高飞行安全性。

02

面临的安全威胁与事件

传统卫星网络因为用户群和卫星供应商不同而采用不同通信体制，同时鉴于卫星终端的稀缺性，安全问题相对较少。

而当前卫星互联网已经成为国家信息基础设施建设和大国在信息时代竞争的关键战略领域，卫星互联网当前面临的数据安全、网络安全问题正在逐渐凸显，特别是以SpaceX为代表的卫星公司把卫星互联网带入大众视野。卫星互联网的泛在性使得越来越多的用户关注卫星互联网安全。全球卫星网络攻击事件呈现几个大趋势：

泛在性：全球卫星网络攻击呈现泛在化特征，2020年以来已发生上百起针对通信卫星、遥感星座及导航系统的定向攻击事件，攻击涵盖信号干扰、协议劫持、轨道欺骗、载荷漏洞利用等多种形式，波及民用通信、气象监测、军事侦察等关键领域。

攻击面扩大：攻击目标从商业企业和军队向科研机构、政府等扩展，针对商业企业和军队以外的安全攻击占比从20%左右提升到40%。

近年来发生的卫星/卫星互联网主要的安全事件，涉及商业、军事、政府等领域。

2025年3月，伊朗油轮发生了严重的卫星互联网安全事件，盛邦安全针对此次事件做了深入剖析，见附件二。

2.1. 美军构建“梅多兰兹”反卫星系统

“梅多兰兹”并非美国太空军在反卫星领域的首次尝试。事实上，它是美军现役卫星通信对抗系统（CCS）的升级版本，即“CCSBlock10.3”。其前代版本“CCSBlock10.2”早在2020年9月就已累计交付14套，并在美太空军的测试中达到了初始作战能力水平。其中，至少有一套已部署于日本冲绳的嘉手纳空军基地。与前代相比，“梅多兰兹”系统进行了轻量化升级，机动性和部署便利性显著提升。其采用的开放式体系结构软件能够通过软件更新增加对不同卫星的干扰能力。此外，该系统还能远程控制三台大型多波段天线，同时执行多项任务，并具备电磁频谱信号数据的监控与记录功能。

图1 美卫星通信对抗系统

“梅多兰兹”系统采用的反卫星技术与当前主流的物理摧毁或致盲手段不同，体现了美国太空军作战理念的变革。其主要针对地球同步轨道上的通信卫星，通过阻塞式干扰技术阻断上行链路的特定频率或频段，涵盖C波段、Ku波段以及军事用途的X波段和Ka波段。

2.2. 俄军全力应对“星链”系统威胁

在俄乌冲突中，“星链”系统对乌军通信能力起到了关键作用，同时也对俄军构成了威胁。为抵消这一威胁，俄军采取了电子战软杀伤结合火力硬摧毁的综合手段。俄军首先利用地面电子战系统，对“星链”系统实施电子干扰。造成“星链”终端通信延迟或服务中断，影响乌军指挥通信。其次，俄军通过监测“星链”终端的电磁辐射信号，定位乌军指挥所，进而引导炮火覆盖乌军指挥所。此外，俄军还开发了“星链”终端专用探测装备，探测和确定“星链”终端位置，为火炮打击提供精确引导。

同时，俄军利用“星链”信号盲区营造干扰带，切断乌军无线通信手段。并且，俄军通过部署“佩列斯维特”激光武器系统等反卫星武器，对“星链”系统实施威慑。在空间对抗方面，俄军研究采用同轨伴飞的空间电子战系统对抗“星链”系统，并发射了多颗监察卫星，用于监测和干扰“星链”卫星的通信或侦察行动。俄军还计划建造自己的“球体”卫星群，以提供通信、导航、遥感及物联网等多种能力，增强在空天信息作战领域的实力。

2.3. “星链”用户终端遭黑客攻击

2022年8月，比利时鲁汶大学的安全研究人员Lennert Wouters在拉斯维加斯Black Hat安全大会上揭示了“星链”用户终端（即相控阵碟形天线）的安全缺陷。Wouters设计了一款仅售25美元的定制电路板（modchip），通过故障注入攻击绕过了星链的安全保护机制，成功侵入系统并运行自定义代码。尽管SpaceX公司已通过更新加大了攻击难度，但Wouters认为除非开发全新版本的主芯片，否则问题无法从根本上解决。

2.4. Garmin卫星定位生产商遭受攻击事件

这是一起卫星产业供应链攻击事件，2020年7月全球知名的卫星定位生产商Garmin遭到WasedLocker勒索软件的攻击。黑客通过加密Garmin的大量系统数据，导致其云服务及定位服务一度无法使用，给全球用户带来了极大的不便。Garmin在其官方声明中证实了遭受网络攻击的事实，并表示没有证据表明任何人在事件期间未经授权访问了用户数据。然而，为了尽快恢复服务，Garmin最终向网络犯罪分子支付了赎金以获得解密工具。

2.5. 美国NASA的供应链攻击事件

2020年12月，APT组织通过供应链攻击将恶意后门植入到SolarWinds的Orion软件更新中。由于SolarWinds的软件被广泛应用于全球各地的政府、企业和组织，因此该后门被超过1.8万名SolarWinds客户下载，导致了大规模的安全事件。其中，包括美国航空航天局（NASA）在内的多个美国联邦政府机构和非政府组织受到了影响。据美国国家安全局（NSA）和美国国家情报总监办公室（ODNI）的声明，此次攻击由俄罗斯外国情报局（SVR）策划。

2.6. Viasat卫星网络攻击事件

针对Viasat的KA-SAT网络事件[1]发生在2022年2月24日，也就是俄罗斯打击乌克兰的同一天。根据Viasat的事件摘要，当天大量集中的恶意流量使许多调制解调器难以保持在线，首次检测到有针对性的卫星通信拒绝服务攻击，流量来自多个SurfBeam2和SurfBeam2+调制解调器和/或物理地址位于乌克兰境内的相关客户端设备。随着调查的深入，幕后的更多细节逐步披露。

此次攻击针对的是美国Viasat电信公司的网络系统，攻击者以卫星通信网络的地面部分为目标。他们利用配置错误的VPN获得了访问权限，并横向移动到KA-SAT卫星网络的管理部分。随后，攻击者执行命令来清除调制解调器的存储空间，导致数以万计的SATCOM调制解调器被毁坏。这次攻击不仅影响了Viasat电信公司的正常运营，还对欧洲多个国家的互联网服务造成了重大影响。

卫星互联网作为新兴技术，其安全挑战也在不断升级。黑客、国家间竞争以及其他恶意行为的威胁对卫星系统都将构成持续性风险。这些威胁可能来自地面、空中或太空，对卫星互联网的正常运行构成严重威胁。

03

卫星互联网安全防护

卫星互联网是一个互联网接入服务网络，逻辑上说，互联网的任何一个节点都可以访问卫星互联网的IP资产，黑客可以通过暴露在互联网的服务节点渗透到卫星互联网的运控服务、测控服务甚至劫持和控制星座卫星。防护面的扩大使得卫星互联网的安全防护成为了一个非常复杂的系统工程。

卫星互联网安全防护涉及的内容很多，本文主要从卫星自身的物理安全、通信链路安全、运维网络安全，构成卫星互联网的三个实体安全：包括卫星载荷、地面信关站和卫星终端安全，以及卫星互联网暴露面管理的两个方向：IP资产发现和漏洞挖掘等八个方面进行论述。

3.1. 卫星的物理安全

3.1.1. 防碰撞 [2]

3.1.1.1. 航天器碰撞的原因

2021年7月和10月，美国太空探索技术公司发射的星链卫星先后两次接近中国空间站，导致中国空间站采取紧急避碰措施。太空如此广袤，为何也会出现太空碎片碰撞这种情况？

图2 地球的太空环境

太空虽然广袤，但自然法则无法违逆，空间物体近距离交会无法避免。

在地球非球形、海洋潮汐、大气阻尼、日月等天体的作用下，绕地球运行的空间物体轨道始终处于缓慢变化之中。根据干扰力的性质不同，轨道变化分为周期性变化和长期变化。轨道缓慢变化，高度相近的空间物体存在近似周期性的接近，称之为“近距离交会事件”。

干扰力的存在给精确预报轨道带来困难和挑战。尤其是在太阳活动的扰动下，难以准确预计低地球轨道上的大气密度环境，导致空间碎片预警工作中的虚警和漏警问题。所谓“虚警”，就是高估了两空间物体的交会风险，引发不必要的避碰工作，既浪费航天器宝贵的燃料，又影响正常的卫星观测任务等工作开展。“漏警”指低估了空间物体的交会风险，使航天器或航天员处于极度危险之中。

太空已经变得很拥挤，广袤的空间一去不复返，碰撞后果不堪设想。机构间空间碎片协调委员会（IADC）关于空间碎片的定义是：人类航天活动产生的、在轨无效的空间物体。不断增多的空间碎片，使得地球轨道资源拥挤不堪，对在轨航天器的安全运行产生威胁。尺寸在厘米级及以上的空间碎片撞击，可导致航天器穿孔甚至解体，直至彻底损坏。厘米级及以下的空间碎片撞击，可导致航天器部分功能受损或失效，关键部件的受损也可能引起整星失效。

1992年美国航天飞机亚特兰蒂斯号，在505公里高度运行了11个月，返回后发现太阳能帆板存在2000余个碰撞点，碎片在舷窗上留下撞击孔，部分已穿透铝制隔板。1996年法国Cerise卫星的重力梯度杆，被Ariane卫星爆炸产生的碎片撞击损坏，卫星姿态失控，最终报废；2009年2月10日，美国铱星33和俄罗斯宇宙2251两卫星发生在轨碰撞事件，卫星解体产生10厘米以上空间碎片数量超过2000件。

3.1.1.2. 碰撞预警及风险识别

这么多的碎片如何监测?众多的空间物体在围绕地球的轨道上运行，为掌握它们包括轨道信息在内的运行状态，需要借助地面观测站、星载雷达和望远镜等设备对空间物体进行跟踪观测，称之为编目工作。

空间物体的编目工作，可比作公安机关的户口管理，每个空间物体从“出生”起都会被赋予唯一的身份识别号码。履行空间物体管理职责的是各航天大国的空间监视部门，比如美国的空间监视网、俄罗斯的空间监视系统等等。限于监测设备的探测能力，现阶段编目工作通常仅对尺寸大于等于10厘米的空间物体进行稳定跟踪，周期性更新其轨道数据。随着空间物体数量的快速增长，解体事件和巨型星座等产生的大量相似轨道空间物体，给编目工作带来了巨大挑战，需要同步提升跟踪探测和数据处理能力以应对挑战。

碎片监测到了，又该如何评估是否有碰撞风险呢？

航天器日常碰撞预警工作是预警规避的基础，当识别到重要空间资产的碰撞风险超过规避阈值时，通常采取轨道机动规避碰撞。

空间物体的碰撞风险识别常会用到“碰撞概率”和“盒子方法”两种方法描述。轨道预报误差不可怕，掌握误差分布统计学规律后，可以使用误差球来描述空间物体可能出现的位置，如使用3倍标准差，使空间物体落在误差球内的概率会控制在99.73%。如果预测的两个空间物体所在的误差球，没有发生交会，则二者的碰撞概率近似为零，如果两误差球有重叠，则对重叠区域的概率密度进行积分，就会得到碰撞概率，这就是碰撞概率的描述方法。因为在卫星运行的沿速度、指向地心和垂直轨道面三个方向，作用力模型掌握的精确程度不同，相应三个方向的预测误差也不同，所以误差球一般使用椭球来描述。盒子方法也正是利用预测误差的这一规律，以航天器为中心，在三个方向上取不同的长度，画出一个长方体的盒子表示交会风险等级。

3.1.1.3. 追踪和预测太空垃圾

监测太空垃圾和跟踪地球太空飞行物体并非易事，需要采用一系列先进的工具和技术来密切监视太空环境。这些工具使他们能够预测物体的轨迹、评估潜在风险并采取必要措施保护免受任何迫在眉睫的威胁。

这项监视的一个关键组成部分是空间碎片跟踪，这需要从各种来源收集数据，这些来源包括：

地面雷达系统：全球各地的雷达站都能够探测太空中的物体并测量其速度和轨迹。这些雷达站对于追踪活跃卫星和碎片的位置至关重要。

太空监视网络：美国空间监视网络(SSN)等组织跟踪轨道上的物体并提供有关其运动以及可能与地球静止轨道卫星发生碰撞的路线的宝贵数据。

专业空间碎片目录：飞行动力学团队依靠最新的数据库，例如太空轨道地球同步轨道目录，追踪地球静止轨道上所有已知物体，包括功能性卫星和碎片。

3.1.1.4. 太空轨道地球同步轨道目录

太空轨道地球同步轨道目录是监测太空垃圾的重要资源，该目录跟踪并记录了地球静止轨道带中所有已知物体。它包括所有已编入目录的太空垃圾和活跃卫星的详细信息。这份综合清单不断更新，包含任何新碎片或卫星轨道变化的实时数据。

查看该目录可识别可能对卫星构成威胁的任何物体。在某些情况下，碎片的轨迹可能不确定，或者可能无法完全预测，这就要求特别警惕。通过将目录中的数据与雷达和太空监视网络相结合，可以对潜在碰撞做出高度准确的预测。

3.1.1.5. 评估和应对碰撞风险

一旦发现潜在威胁，就需要评估风险的严重程度。通过评估太空垃圾的大小、速度和轨迹等因素，以确定发生碰撞的可能性。即使是小碎片，其速度高达每小时28,000公里，也可能对卫星造成严重损害。在某些情况下，碰撞可能会完全摧毁卫星或使其无法运行，从而导致关键服务能力的丧失。

如果确认风险很大，就需要采取行动。这通常涉及规划防撞机动——这个过程需要精确的计算和仔细的协调。这些机动可能涉及微调卫星的轨道，重新定位卫星，使其脱离预测的碰撞路径。

虽然操纵卫星很复杂，而且燃料和资源成本高昂，但这是避免潜在灾难性后果的必要预防措施。快速有效的响应能力能确保卫星保持运行，避免服务中断。

由此可见，保护卫星免受太空碎片影响，需要通过先进的跟踪系统、预测模型和快速响应策略，确保卫星能够不间断地执行任务，从而为太空基础设施的稳定性和可靠性做出贡献。

3.1.2. 安全销毁

卫星互联网的快速发展导致地球轨道上卫星数量的急剧增加。虽然这些前所未有的巨型卫星星座可能带来重要的商业利益，但是这些卫星会导致轨道碎片的显著增加。

对于达到使用寿命的人造卫星，通常有两种处理方式：一是提升其运行轨道至更高的“墓地轨道”，以避免对其他卫星造成干扰；二是降低其飞行高度，使其再入大气层并烧毁。对于低轨卫星而言，后者是更为常见的选择。

在再入大气层过程中，一些卫星部件会在大气层摩擦高温下幸存并落回地球。现代空间碎片法规要求避免这种事件，不受控制的再入过程造成地面人身伤害的几率应小于1/10000。

从很多观测中发现，卫星主体通常在70-80千米的高空解体，随后内部组件分散开来。有可能幸存的物体包括高熔点材料（如钛合金或不锈钢）制成的推进剂箱，以及高密度物体，如光学仪器和大型机械装置。研究人员正在研究如何使这些物体更容易销毁，例如，使用新型铝合金材料制造燃料箱。然而，如果没有足够早地暴露在高温中，即使重新设计的部件也不会熔毁。卫星销毁需要采用整体方法，如使卫星在再入大气层过程中尽早解体，使用各种软件模拟评估卫星设计的可破坏性，模拟再入大气层过程并开展物理试验。

卫星销毁还有一些其他的方法，包括：以受控方式使卫星坠落，关闭老化卫星使其不易发生爆炸，采用新技术使卫星更轻或更高效，保留燃料以进行安全地废弃处理等。

3.2. 卫星链路安全防护

卫星链路是开放链路。如何安全的利用这样的开放链路，为不同用户和组织提供安全的通信服务，是卫星互联网亟待解决的问题。

3.2.1. 空口公共信道的网络隔离与切片

卫星互联网提供全球泛在用户的互联网接入服务，需要实现不同用户的网络隔离，实现不同业务的服务切片。这需要充分考虑天地一体化信息网络的网络架构、路由交换体制、网管网控模式以及系统业务类别及每类业务对服务质量的要求，将传输与安全有机融合进卫星通信网络安全架构设计。安全保密架构需要考虑网内运维运控的安全保密、地面网安全互联互通、不同用户共用等三个方面的特点，且具有一定的弹性、灵活性，以及较高的抗毁特性，支持对不同安全域用户或业务的针对性安全防护与定制化保密需求。

3.2.2. 针对卫星通信多层次的安全保护

针对卫星通信的特点，开展物理层、链路层、网络层到应用层等各个层面的安全保密需求分析与一体化设计。卫星通信协议（包含网络控制相关协议、业务层面协议等）不同于地面通信网络协议，需要保护的业务安全需求与地面网络有较大的差异，需要研究针对性的安全防护技术。

针对卫星通信的物理层，需要解决通信抗干扰问题，可以通过跳扩频技术、相控阵技术、激光通信等指向性强的通信技术，实现物理层的安全防护。

针对卫星通信链路层，需要解决网络控制、接入控制、入网认证等安全风险。

针对卫星通信网络层，需要解决网管信息、路由信息、用户业务网络的安全防护。

需要解决网络集中化安全管理问题，包括卫星信号传输时延长、连接时间不连续、不能提供实时在线安全管理，安全管理措施必须适应延迟长、非对称、不连续的卫星信道特点。

由于星载设备计算能力、存储能力及能量有限，可维护性也较差，需要开展基于受限星载处理能力情况下的安全保密功能设计与星地功能分配。

3.2.3. 星地协同的认证鉴权技术

卫星互联网网络拓扑结构的动态变化使得拓扑结构和节点间信任关系的维护变得复杂，路由特征、用户寻址等都会发生变化，使得地面相对静态的安全措施不适用于这种动态变化，需要解决切换认证与位置管理安全等问题。这种动态变化的网络特性给传统认证协议带来了挑战，需要设计高效、轻量级的认证鉴权算法与协议，降低在接入过程的信息交互次数，提高协议效率。

需要借鉴现有地面移动通信网络，充分考虑各类业务的特点，研究适合星上处理、星地协同的轻量化认证鉴权方法，设计认证鉴权参数数量和长度，实现认证鉴权流程与通信流程一体化设计，满足卫星通信网络中终端、卫星、应用等各个实体分区分域信任、接入认证、动态切换授权等认证授权需求。

3.3. 运控网络的安全防护

3.3.1. 卫星互联网运控网络

运控网络：用于卫星互联网的运行维护，以及卫星资源、链路资源、网络资源调度和控制的网络。

简单的说，就是卫星互联网的运维网络。运维的主要工作即通过高效的业务管理、状态监测、通信设备及网络设备的管理以及网络能力的优化等，实现高效的网络性能管理，从而保障星座系统自身的稳定运行以及对外的稳定服务。

1）采用测控网络实现网络运维

早期卫星网络的运维管控是通过地面测控系统完成的，受限于测控站建设敏感性和卫星测控频段用户密度等，地面测控网无法实现对低轨卫星的全时段观测。考虑到信关站馈电链路速率高、全球布站的优势，通过联合测控系统能够保证遥测数据24 小时无缝回传，为卫星故障处置提供基本的遥测数据支撑。

2）建设独立的运控网络

利用卫星通信信道和地面线路，独立构建运控网络，实现对卫星、网络的运维控制。这种方式能将控制面和业务面完全分割，安全性好，运维效率高，但是成本很高。

3）建设逻辑的运控网络

采用VPN技术，通过Overlay的方式，在卫星互联网上，建设出一个逻辑隔离的运控网络。这种方式成本低，相对灵活，但是安全性需要加强保障。

3.3.2. 运控的网络安全

运维网络的安全主要是要保障与业务网络的隔离，通常采用VPN在业务网络上构建一个逻辑上隔离的运控网络，同时使用防火墙加以安全防护。

可以采用零信任安全技术，进一步减少暴露面，持续监控并授权使用运控网络，可以提高运控网络的安全性。

以星链为例，其运控网络需要通过POP节点连接在一起，且所有的运维服务都放在云上，所以POP节点的安全防护和云端的安全防护需要重点关注。

3.3.2.1. POP节点安全

卫星互联网地面网络中的互联网POP（Point of Presence）节点处于非常关键的位置。它是卫星网络与地面互联网连接的重要交汇点。从宏观网络拓扑结构来看，卫星链路将数据传输到地面的POP节点，然后POP节点再将数据分发到各种地面网络，如企业网络、家庭宽带网络等。POP节点的安全防护主要包括：

1）物理安全保障

POP节点包含众多网络设备，需要有可靠的物理防护措施。要设置在具备良好安保条件的场所，通过门禁系统、监控摄像头等防止非法人员的闯入破坏，同时要做好应对火灾、洪水、地震等自然灾害的防范准备，确保机房等设施的稳固安全，保障设备能正常运行。

2）网络访问控制

严格限制对POP节点的网络访问，只允许授权的IP地址或网络区域的设备与之通信连接。采用访问控制列表（ACL）、防火墙等技术，对外来流量进行筛选过滤，阻止非法的访问请求，防止黑客等恶意势力利用漏洞入侵节点，篡改网络配置、窃取数据等。

3）数据安全防护

对于经过POP节点转发和处理的数据，要确保其完整性和保密性。运用加密技术对数据进行加密传输和存储，并且通过数据校验、数字签名等手段保证数据在传输过程中未被篡改。同时，做好数据备份工作，防止设备故障、攻击等导致数据丢失，以满足业务连续性的要求。

4）设备可靠性与冗余

POP节点内的路由器、交换机等关键设备应具备高可靠性，采用冗余设计，如配置双电源、备用设备等。当一台设备出现故障时，能迅速切换到备用设备继续工作，减少网络中断的时间，确保卫星互联网服务的稳定性，避免对大量用户的使用造成影响。

3.3.2.2. 云端服务安全

大型卫星星座也会使用云资源构建管理运维网络。在云端使用各类服务网元和安全网元对业务数据、运维数据和管理数据进行处理和防护。主要安全需求包括：

1）数据隐私保护

云端存储着海量的卫星互联网用户数据、业务数据等，要严格保护数据的隐私。采用加密算法对数据加密，无论是在存储状态还是传输过程中都确保其保密性，同时遵循严格的数据访问规则，只有经过授权的用户或业务模块才能访问特定的数据，防止数据被泄露给无关方。

2）资源隔离保障

在云端要实现不同用户、不同业务之间的资源隔离。通过虚拟化技术等手段，确保各用户使用的计算资源、存储资源等相互独立，防止因某个用户或业务遭受攻击、出现故障而影响到其他用户和业务的正常运行，保障云端服务的稳定性和安全性。

3）安全漏洞管理

定期对云端服务所依托的软件、系统等进行安全漏洞扫描和检测，及时发现可能存在的漏洞隐患，并迅速安排修复补丁等处理措施。同时，建立应急响应机制，一旦出现安全事件，能快速反应并采取有效的应对措施，降低事件对云端服务和用户的影响程度。

4）合规性要求满足

要遵循相关的法律法规和行业标准，比如数据保护法规、网络安全法规等，确保云端服务在数据存储、处理、传输等各个环节都符合相应要求，做好用户数据的合法合规管理，避免因违反规定而面临法律风险，维护卫星互联网云端服务的健康有序发展。

3.3.3. 运控网络的运维安全

1）采用统一的运维接口并审计

为了保障网络和数据不受来自外部和内部用户的入侵和破坏，通常使用堡垒机这样的技术手段监控和记录运维人员对网络内的服务器、网络设备、安全设备、数据库等设备的操作行为，以便集中报警、及时处理及审计定责。

通过身份准入控制策略与动态权限管理机制，实现对人员访问资产的精细化管控，依托实时监控与敏感操作拦截技术强化访问过程风险阻断，同时基于全链路操作日志记录与多维度审计分析系统，完整追溯用户在资产内的行为轨迹与指令变更。

2）人员管理与操作规范

对于参与卫星互联网运维的工作人员，要进行严格的背景审查和权限分级管理。只有具备相应资质、经过专业培训且通过安全考核的人员才能参与关键操作，防止因人为疏忽或恶意行为引发安全问题。例如，只有高级别权限的工程师才能对卫星的轨道调整指令进行下达操作。

制定详细且标准化的操作流程和规范手册，运维人员在进行设备巡检、参数配置、软件升级等日常工作时，必须严格按照流程执行，避免出现误操作影响卫星互联网系统的正常运行。

3）系统监控与故障预警

搭建全面的监控体系，对卫星、地面站、通信链路等各个环节的运行状态参数，如信号强度、设备温度、电量等进行实时监测。一旦出现异常数据，能够及时发出警报，以便运维人员快速定位和排查故障。比如，当卫星通信模块温度过高时，监控系统立刻发出高温预警，提醒运维人员采取散热等相应措施。

具备智能的故障预测能力，利用大数据分析、机器学习等技术，基于历史运行数据来预判可能出现的故障隐患，提前做好预防和应对准备，降低故障发生概率和影响程度。

4）应急响应机制

制定完善的应急预案，明确不同故障场景、安全事件下的应对流程和责任分工。例如，当遭遇太阳风暴等空间天气事件导致卫星通信中断时，各部门清楚知晓自己应采取的行动，快速恢复通信链路。

定期开展应急演练，确保运维人员熟悉应急流程，提高应对突发事件的实际操作能力，保障在紧急情况下能高效地解决问题，减少对卫星互联网服务的影响。

3.3.4. 资产安全

1) 资产识别需求

要精准识别卫星互联网中各类资产，包括卫星本体、地面控制站、信关站、互联网接入节点、用户终端等硬件设施，明确其型号、性能、所处位置等关键信息，以便清楚掌握整体资产布局情况。

对于相关软件系统，像卫星的操作系统、控制软件、通信协议等也要准确识别，清楚了解软件版本、功能特点等，知晓可能存在的薄弱点。

2) 漏洞监测需求

持续监测卫星互联网资产可能存在的漏洞，不管是硬件方面因制造工艺等产生的物理漏洞，还是软件因代码编写等导致的逻辑漏洞，都要及时发现。如卫星通信链路加密机制是否存在被破解风险等，要能监测出来。

对新发现的漏洞要能快速评估其严重程度，判断是否容易被攻击者利用从而威胁整个卫星互联网的安全运行。

3) 态势感知需求

实时感知卫星互联网资产面临的安全态势，了解是否遭受外部恶意攻击，例如是否有非法信号试图干扰卫星通信、是否有黑客尝试入侵地面控制站等情况，及时掌握整体安全状况的动态变化。

能基于历史数据和实时监测信息预测可能出现的安全威胁走向，提前做好应对准备，保障资产安全稳定运行。

4) 数据保护需求

对于卫星互联网运行中产生和传输的各类数据，像卫星遥感数据、用户通信数据等，要确保其保密性，防止数据被不法分子获取利用。

保证数据的完整性，避免数据在传输和存储过程中被篡改，影响到卫星互联网各项业务的正常开展。

5) 合规需求

要确保卫星互联网资产的运营管理等符合国内国际相关的安全法规、标准，例如无线电频率使用、卫星轨道部署、安全及隐私保护要求要符合相关规范等，避免因违规带来安全风险和法律问题。

3.4. 卫星载荷的安全防护

3.4.1. 卫星测控的安全防护

测控域涉及卫星平台、测控站和卫星操作中心，以及它们之间的通信链路。在实际部署中，还可能会借助第三方的测控站。因此，测控域安全至少包括以下特性：测控载荷与测控地面系统间的认证、遥控数据的机密性和完整性保护、遥测数据的机密性保护、测控站安全防护、卫星操作中心安全防护。

要对卫星的遥测遥控信息进行安全防护，最有效的方法就是对其进行加密处理，以防止测控信息资源被故意地或偶然地非授权泄露、更改、破坏，或使信息被敌方辨识和控制，从而确保测控信息的完整性、保密性、可用性和可控性。

3.4.2. 星载通信载荷的安全防护

在卫星通信载荷安全方面，需要应对通信链路干扰、信号窃听、信号劫持、信号欺骗等威胁。其中，链路干扰是指在卫星通信过程中，由于电磁波干扰、人为干扰等原因，导致卫星通信链路出现故障或中断；信号窃听是指攻击者通过非法手段获取卫星通信链路中的信息，从而窃取机密信息；信号劫持是指攻击者通过非法手段控制卫星通信链路，从而篡改或伪造通信信息；信号欺骗是指攻击者通过伪造卫星通信链路中的信息，从而欺骗接收方，使其做出错误的决策。

针对这些威胁，可以采用加密技术、身份认证技术、安全路由技术等手段进行防护。例如，在通信链路中，可以采用加密技术对数据进行加密传输，防止信号窃听和信号劫持；在信号传输过程中，可以采用身份认证技术对信号进行验证，防止信号欺骗。此外，还可以采用安全路由技术，确保卫星通信链路的安全性和可靠性。

3.4.3. 星载网络载荷的安全防护

随着卫星通信技术的发展，网络路由器和交换机也放到了星上，被称为星载网络载荷。从网络本身的角度来说，网络载荷同样面临安全威胁。

03 卫星互联网安全防护

卫星互联网在组网层面的威胁主要来自对星座网络结构的物理破坏和对路由的攻击。星座结构破坏旨在永久破坏卫星节点，改变网络的物理拓扑结构，使网络链路在短期内断开连接，无法修复。根据威胁的产生，物理破坏可分为人为破坏和非人为破坏。人为破坏是有目的地、主动地攻击目标节点，旨在降低网络的连接性，典型的攻击如使用弹道导弹和激光武器对卫星进行物理摧毁等。网络的关键节点更容易被优先作为攻击目标，从而最大限度地降低网络的可用性。非人为破坏是由环境威胁造成的，如节点被随机销毁。一方面，超密度轨道飞行器和空间碎片之间存在碰撞的风险，轨道飞行器需要依靠轨道环境态势感知技术来避免碰撞。另一方面，高能电磁辐射会导致航天器电子设备出现故障，如系统关闭或电源中断。如果被破坏的节点不重要且数量较少，则网络可以重建被破坏拓扑的路由。然而，随着被摧毁节点数量的增加，一些相邻卫星之间的距离将超过通信范围，网络将在物理上被划分为孤立的多个子网络，消息也无法在子网络之间传递。

星座结构破坏的后果是物理拓扑结构的变化，因此这种威胁一旦发生就很容易观察到。与摧毁卫星不同，路由攻击是在信息空间对路由协议的破坏。路由攻击通常可以分为内部攻击和外部攻击。在内部攻击中，卫星节点可以被捕获并控制，而在外部攻击中，攻击者无权访问网络，攻击可以针对路由发现、数据传递和路由维护的过程。路由攻击可能导致不必要的路由发现请求、添加无效的路由、增加数据包丢失、更改网络拓扑以及耗尽网络资源，让消息“迷失”在浩瀚星空。

针对路由的另一典型攻击是路由信息欺骗。攻击者只通过发布虚假拓扑信息来欺骗网络节点，而不会对节点进行物理破坏。路由信息欺骗可以分为路由节点伪装和逻辑网络分割。为了实现路由节点伪装，恶意节点需要通过篡改或伪造路由信息来声明自己是最佳转发节点，以拦截或收集网络中的消息。黑洞攻击和虫洞攻击是两种常见的节点伪装攻击。以黑洞攻击为例，攻击者向目的地广播最便宜或最短的伪造路径，接收节点选择通过攻击者的路径，然后攻击者可以随意分析甚至丢弃这些数据包。

3.5. 地面信关站的安全防护

地面站信关站是整个卫星互联网系统的重要组成部分，它们负责在卫星与地面互联网骨干网络之间传输数据。地面信关站通过卫星通信，将从用户终端发送和接收的数据引导至全球互联网主干网，确保整个系统的正常运行。由此可以看出，地面信关站的安全防护是非常重要的。

3.5.1. 地面信关站主要组成

主要以星链为例，一个典型的地面信关站的主要构成包括：

1) 天线系统

相控阵天线：地面站使用相控阵天线来与低地球轨道（LEO）上的Starlink卫星通信。相控阵天线可以通过电子方式调整波束的方向，而不需要物理旋转天线，能够更快地跟踪移动的卫星。

Ku波段和Ka波段支持：天线支持Starlink使用的Ku波段(10.7-12.7GHz下行，14.0-14.5GHz上行)和Ka波段(17.7-20.2GHz下行，27.5-30.0GHz上行)，从而实现高速的数据传输。

2) 射频设备

功率放大器：用于增强从地面站到卫星的上行信号，确保在大气层中传输时信号的稳定性和质量。

低噪声放大器（LNA）：接收卫星发送的信号，并在信号处理之前进行初步的放大，确保接收到的微弱信号能够被有效处理。

信号转换器：负责将来自用户终端的低频信号转换为适合Ku和Ka波段的高频信号，用于与卫星的通信。

3) 网络和数据处理设备

路由器和交换机：地面站需要高速路由器和交换机来管理大量的数据流量，将来自卫星的数据引导到全球互联网，并处理从互联网发送给卫星的请求。

数据服务器：负责存储和处理从卫星接收到的数据，同时管理地面站与互联网主干网的连接。服务器的处理能力需要能够应对高并发的大量数据传输需求。

4) 基础设施

建筑和支持设施：包括天线的物理安装结构、塔架、信号处理和网络设备的机房、冷却系统、电力供应系统等。确保这些设施能够正常运行，保持持续的信号处理和互联网连接。

5) 安防系统

地面站通常位于偏远地区，需要配备监控和安保措施，以保护设备免受破坏和未经授权的访问。

6) 电力系统

主电力供应：通常地面站与电网相连，获得持续的电力供应。

备用电力系统：为了防止停电影响运行，地面站通常配备备用发电机和不间断电源(UPS)，以在紧急情况下提供电力。

7) 冷却系统

气候控制：由于地面站内部的电子设备和服务器在运行时会产生大量的热量，必须有冷却系统来控制设备的温度，防止过热导致的故障。通常会采用空气冷却或液体冷却系统。

8) 网络连接

光纤连接：地面站与全球互联网主干网络的连接通常通过高速光纤进行。光纤网络可以提供超低延迟和高带宽的传输，确保Starlink系统能够实时处理和传递大量的网络数据。

9) 备份和冗余设施

冗余系统：为了确保可靠性，地面站通常会部署多套冗余设备，包括天线、功率放大器和网络设备，以便在某一部分设备故障时能够无缝切换到备用设备，避免通信中断。

10) 管理和监控系统

远程监控和控制：地面站配备了先进的监控和管理系统，能够实时检测设备状态，进行远程维护和故障排查。地面站的运营中心可以通过这些系统掌握整个网络的运行情况。

自动化运维：通过自动化管理平台，地面站可以自动处理某些常见故障，减少人为干预和维护成本。

3.5.2. 信关站的安全防护

1) 物理安全防护

要防止非法人员的物理入侵，通过设置严格的门禁系统、监控设备、安保巡逻等措施，确保只有授权人员能够进入地面信关站所在区域及机房内部，避免设备被破坏、篡改等情况发生。

做好应对自然灾害的准备，如建设具备抗震、防洪、防火等能力的基础设施，保障在地震、洪水、火灾等状况下信关站能正常运行或者尽可能减少损害。

2) 网络安全防护

要防范网络攻击，包括来自外部的黑客入侵、恶意软件植入等。通过部署防火墙、入侵检测系统、防病毒软件等，实时监测并阻断可疑的网络连接和恶意程序，防止信关站网络被攻破，导致数据泄露或运行故障。

做好数据加密工作，对信关站传输和存储的数据，无论是控制指令还是业务数据等，都采用高强度的加密算法进行加密处理，确保即使数据被截取，攻击者也难以获取真实信息。

3) 通信安全防护

保障通信链路的稳定性和可靠性，防止信号干扰、窃听等情况。采用抗干扰技术，提升卫星与信关站之间通信信号的质量，同时利用通信加密等手段，杜绝通信过程中信息被窃取监听的可能。

做好身份认证管理，对连接信关站的各类设备、用户等进行严格身份验证，只有通过认证的才能建立通信连接，防止非法设备接入，干扰正常通信秩序。

4) 电力供应安全防护

配备可靠的电力供应系统，有主电源、备用电源（如不间断电源UPS、柴油发电机等），确保在停电等突发状况下，信关站能持续获得电力支持，维持正常运转，避免因断电引发的数据丢失、设备损坏等问题。

对电力供应线路等做好监测维护，及时排查线路老化、故障隐患，保障电力输送的顺畅安全。

5) 运维管理安全防护

制定完善的运维管理制度和操作规范，对工作人员的操作流程、权限分配等严格管控，防止因人为失误或者违规操作给信关站带来安全风险。

做好运维审计，记录工作人员的操作行为等信息，便于事后追溯和排查可能出现的安全问题，及时采取补救措施。

3.6. 卫星通信终端的安全接入

3.6.1. 多通信链路探测切换

考虑到卫星通信网络的动态性，卫星服务商覆盖的地球区域不同，同一个服务商各个卫星覆盖的地球区域不同，机载/船载/车载卫星通信终端环境一般需要放置多个卫星天线，随着空间位置移动，调度调整到合适的服务商和卫星。此外，卫星通信终端可能运行在Internet、MPLS、LTE、5G等广域网链路并行的环境。

卫星通信终端需要支持多链路，及多链路按需动态选路能力。在卫星交叠覆盖区域，采用多路负载实现带宽的充分利用，链路质量探测，自动调整链路优先级和负载比例。在卫星覆盖临界区域，链路质量探测，自动切换路由。当卫星通信终端接入地面5G网络时，需要解决两种不同网络环境下的安全协议转换、加密方式匹配等问题，以保障终端的安全接入和数据交互安全。

基于链路质量：假设多种应用运行在多条链路上，可自行配置链路丢包、延迟、抖动的阈值等参数，但链路出现异常后，可自动将异常链路上的业务切换至最优链路，保障业务访问体验。

基于业务级别：假设多种应用运行在多条链路上，可自行配置业务优先级及链路匹配原则，实现高优先级业务优先在高质量链路上访问，同时当高质量链路异常后，可无感切换至备用链路，保障业务访问体验和连续性。

基于时间等维度：实现业务在某一时间段内或周期性对高优先级业务进行保障调度，保证业务可靠性要求。

3.6.2. 网络攻击防范

网络攻击形式多样，如DDoS攻击、中间人攻击等，都可能影响卫星通信终端的安全接入。为了防范这些攻击，需致力于开发防火墙技术、入侵检测系统和防病毒软件等专门针对卫星通信环境的防护措施。例如，入侵检测系统可以实时监测卫星通信网络中的异常流量和行为模式，一旦发现疑似攻击行为，及时发出警报并采取措施阻止攻击，确保终端安全接入卫星通信网络，内网防范空口流量攻击。

事前风险监测：能够在事前自动识别网络内主机资产和服务器资产的网络信息，能够识别内网资产的开放端口、弱密码等安全风险，同时提供多种可视化系统监控数据，帮助用户有效监测和预知网络风险。

事中防护响应：具备深入的全方位安全防护能力，包括入侵防护、病毒防护、DOS/DDOS攻击防护、URL过滤、防暴力破解、威胁情报应急响应、APT攻击防护、EDR联动防护等，为用户提供一个多层次防御体系，保障企业和组织的网络安全。

事后追溯审计：事后能够进行追踪溯源、取证分析，根据日志分析事件来源和原因，并进行针对性加固措施；能够通过黑客视角或资产视角对攻击事件进行综合分析，将抽象的网络形象化，将攻击行为可视化，帮助用户快速了解网络的安全情况。同时，基于资产视角，将所有攻击行为深度分解为四个阶段，为用户展示出一条完整的攻击链，帮助管理员对处于不同攻击阶段的高风险资产进行针对性安全加固处理。

管理平台通过收集卫星通信安全接入终端设备安全日志，进行大数据分析，呈现整网安全态势，帮助运维人员提前预警和安全风险诊断。通过丰富的日志、告警、报表等多种形式简化运维，提升运维效率，降低运维成本。全面的安全态势感知可视化，做到一张图就能了解一张网，及时知晓内网接入卫星通信网络各个节点的安全和网络的情况。

3.6.3. 流量安全管控

卫星通信终端网络流量大致分为三种类型：

·业务数据回传，需要考虑对数据进行加密处理。

·办公数据，需要通过VPN方式实现端到端的安全通道，进而实现用户自有数据中心或企业内部网络访问。

·用户个人娱乐访问互联网的网络流量。

业务流量需要进行带宽保障，设置最低专享带宽，实时监测业务流量的带宽使用，在无业务时可释放带宽给用户上网流量，在业务流量的专享带宽的使用率接近阈值时自动扩张专享带宽。上网流量需符合法律规定，对访问的网站、内容进行控制。使用防火墙和上网审计设备实现安全策略管控。

3.6.4. 轻量级加密机制

卫星通信业务流量需经过安全通道传输，保障数据不被窃取，指令不被篡改，使用加密设备保障业务数据安全。业务设备禁止上网，防止安全事件。

卫星通信终端往往受到计算资源和能源的限制，传统的复杂加密机制可能无法高效运行。因此，研究适合卫星通信终端的轻量级加密机制是一个重要方向。这些轻量级加密机制在保证一定加密强度的前提下，能够减少对终端计算资源和能源的消耗。例如，通过简化加密运算流程、采用更高效的密钥管理方式等，使卫星通信终端能够快速、安全地进行加密和解密操作，从而保障安全接入过程中的数据安全。

3.7. 卫星互联网资产发现

通常采用卫星互联网测绘手段来发现卫星互联网资产，通过分析资产情况，减少互联网暴露面，进而减少安全风险。

3.7.1. 卫星互联网测绘的意义

网络空间测绘技术作为国家网络安全和全球网络空间态势感知的基础技术，世界各国都十分重视其理论研究与应用实践。由于网络空间的测绘数据可以反映国家网络安全现状以及加强网络空间态势感知能力，欧美国家纷纷建设网络空间测绘系统，针对整个网络空间进行全方位全天候测绘。攻击者可以通过测绘系统收集目标多维度信息，挖掘目标脆弱面，进一步执行特定攻击，因此，网络空间测绘引入了新的安全风险，来自国内外的未授权或非法的网络空间测绘行为严重威胁我国网络安全。

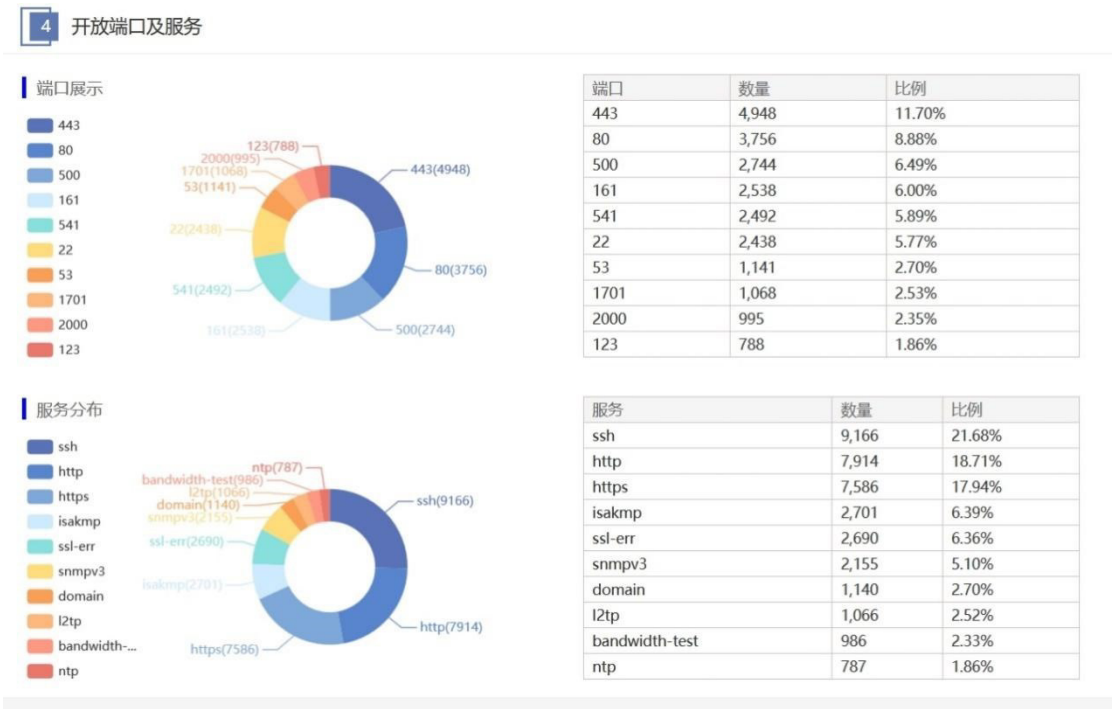
近年来，网络空间测绘行为呈爆发性增长态势，国内外黑客组织、白帽团体、政企机构、军事力量、敌对势力、有特定意图的个人等均在以各种各样的方式开展网络空间测绘、获取各自关注的网络空间底图数据、业务应用数据、舆情信息等。恶意的网络空间测绘行为常常混杂在正常网络流量中，能够造成网络关键基础设施攻击面暴露、重要敏感数据信息泄露、舆情态势被对手掌握等诸多问题，对国家安全危害极大，给我国网络空间安全治理带来极大的挑战。

2021年公布实施的《关键信息基础设施安全保护条例》要求建立健全关键信息基础设施安全保护体系，提升网络安全防护能力。关键信息基础设施一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益。因此面向关键信息基础设施开展网络空间反测绘关键技术研究及应用示范，形成网络空间测绘行为恶意属性甄别能力，从而增强网络空间安全防御措施的针对性和有效性，促进网络空间安全防御能力提升，保护我国关键信息基础设施，保障互联网安全和国家安全。

3.7.2. 卫星互联网测绘情况

采用无状态防溯源探测、高性能端口扫描等技术，以及大规模分布式扫描引擎资源，可实现对卫星互联网网络的高效探测。通过多维度数据关联融合分析技术，精确识别卫星网络资产的归属、行业等信息。智能关联分析资产的归属单位，发现未知或未监控的资产、服务和数据等，全面掌握卫星互联网网络资产情况。将测绘与漏洞检测技术相结合，基于指纹信息精确定位资产漏洞，实现对卫星互联网网络中紧急漏洞的快速评估、响应与全生命周期的监控，保障网络安全。卫星互联网测绘将与人工智能、大数据、云计算等技术进一步深度融合。利用人工智能的机器学习和深度学习算法，可实现对测绘数据的自动化分析和处理，提高测绘效率和精度，挖掘更多有价值的信息。

通过对卫星互联网自治域进行资产测绘，可以掌握IPv4和IPv6资产全球分布情况，统计端口、服务分布规律，展示设备和主机漏洞趋势。跟踪和分析POP点和信关站变化情况，绘制全球POP点和信关站连接关系，标注骨干网络拓扑连接关系。研究和分析卫星互联网架构，采用多种方式获取系统域名，绘制域名和子域名的层级关系。



端口	数量	比例
443	4,948	11.70%
80	3,756	8.88%
500	2,744	6.49%
161	2,538	6.00%
541	2,492	5.89%
22	2,438	5.77%
53	1,141	2.70%
1701	1,068	2.53%
2000	995	2.35%
123	788	1.86%

服务	数量	比例
ssh	9,166	21.68%
http	7,914	18.71%
https	7,586	17.94%
isakmp	2,701	6.39%
ssl-err	2,690	6.36%
snmpv3	2,155	5.10%
domain	1,140	2.70%
l2tp	1,066	2.52%
bandwidth-test	986	2.33%
ntp	787	1.86%

图3 终端测绘端口及服务分布情况

图4 卫星互联网资产操作系统类型

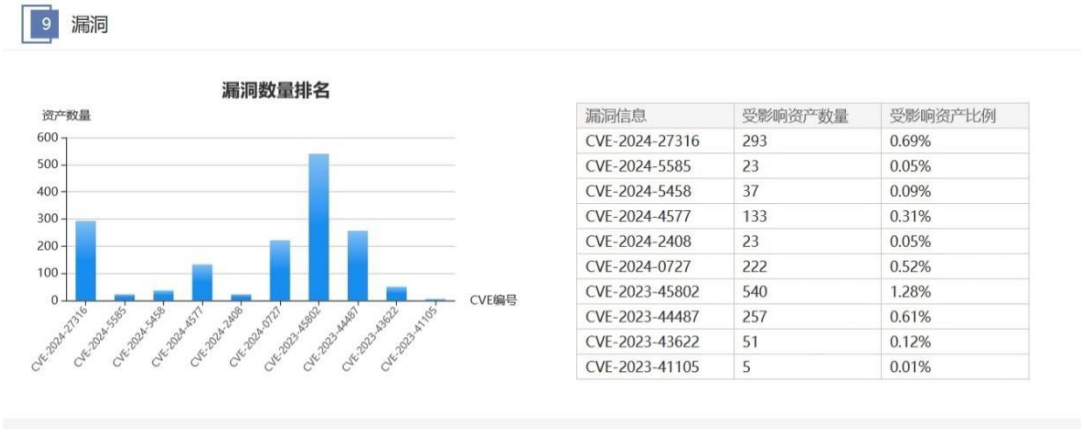


图5 卫星互联网资产漏洞分布情况

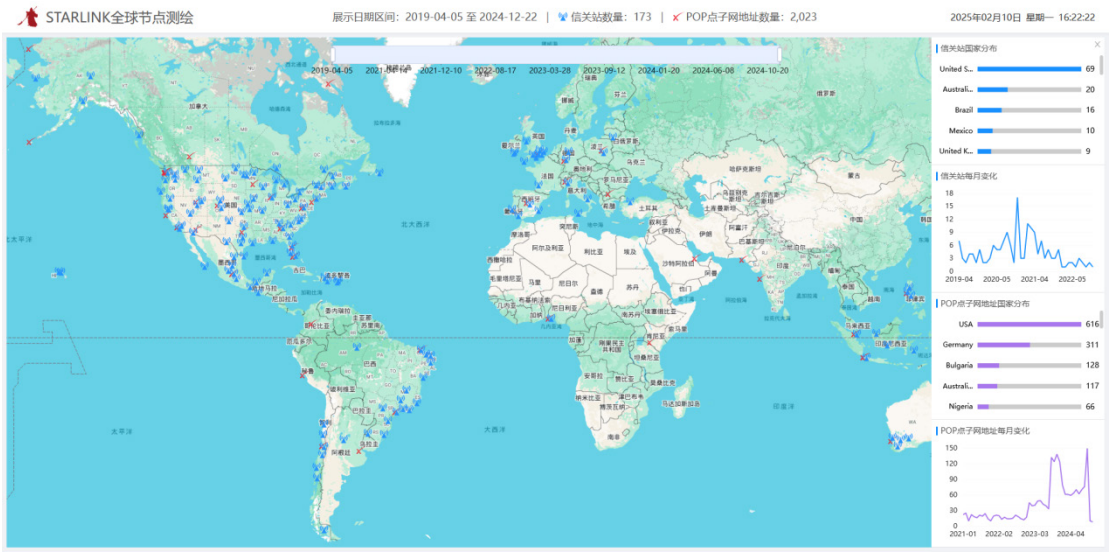


图6 卫星互联网信关站、POP点统计

3.8. 卫星互联网的漏洞挖掘与防护

3.8.1. 卫星互联网通信网络面临的主要安全风险

1）用户数据泄露

由于卫星转发地域的广泛性和无线传输的透明性，大部分卫星通信信息不加密，通信内容近乎“裸奔”，而卫星用户多为政府、大型企业，通过卫星传递的政治、经济、金融、经贸等的重要数据存在泄露风险。对卫星通信信号使用简单设备进行接收分析，就可以解译卫星通信数据，信息内容涉及政治、经济、外交、商贸敏感信息和银行业务、证券交易、石油开采、地质勘探、地震气象等重要数据，用户数据泄露代价很大。

2）用户账户被窃取

使用软件无线电截获平台对卫星无线网络身份进行窃听，实时掌握信号出现规律、物理层时隙规律，分析目标用户行为规律，利用在线用户的空闲时隙，模拟第三方小站用户，实现目标通信网络的接入。传统卫星通信技术体制均存在此类安全风险，轻则产生资费纠纷，重则导致用户通信网络和服务中断。

3）关键设备存在漏洞

供应商打着终身技术支持、提供远程服务、便于升级维护等各种幌子，在关键设备、枢纽部件上有意无意、或多或少的预制后门，留有漏洞。这些后门、漏洞被竞争对手利用，卫星设备安全风险极高。通过对设备固件进行提取分析发现，其小站设备固件软件逻辑中，广泛存在应用控制后门和密码陷门，用于远程登录、管理控制和信息窃取。该后门机制可被第三方利用实施网络攻击，窃取信息和致瘫网络。通常卫星网络入侵，以及在俄乌战争中乌克兰Viasat卫星网络攻击事件就是采取此类方法，存在重大安全隐患。

4）业务带宽被占用

卫星通信存在区域覆盖广泛、下行信号广播式等特点、通信协议存在可篡改漏洞，基于非合作方卫星资源可建立隐蔽信息传输通道。卫星网通信协议安全设计不足，流量可被窃取（带宽占用），导致用户资费流失，服务质量下降等问题。

5）基础设施被渗透控制

“黑客”通过卫星无线网络漏洞对地面网络进行渗透，轻松绕过防护设备，攻击控制测控设备、运控设备及核心服务器等关键基础设施，造成卫星核心设备瘫痪，卫星通信业务无法开展。

3.8.2. 卫星互联网地面网络的漏洞挖掘

3.8.2.1. 互联网POP节点

卫星互联网地面网络中的互联网POP（Point of Presence）节点处于非常关键的位置。它是卫星网络与地面互联网连接的重要交汇点。从宏观网络拓扑结构来看，卫星链路将数据传输到地面的POP节点，然后POP节点再将数据分发到各种地面网络，如企业网络、家庭宽带网络等。例如，对于一个为偏远地区提供卫星互联网服务的系统，POP节点负责接收卫星信号，并将互联网服务延伸到当地的各个社区网络。

POP节点是实现卫星互联网覆盖的关键设施，能够为用户提供高速、稳定的互联网接入服务。

POP节点的布局通常考虑到地理覆盖范围和用户密度等因素。在人口密集地区，可能会有多个POP节点以满足大量用户的需求。而在偏远地区，一个POP节点可能覆盖较大的地理区域，虽然用户数量相对较少，但对于保证该地区的网络连通性至关重要。且POP节点承担着数据汇聚的功能。来自卫星链路的多个用户的数据流量在POP节点汇聚。例如，不同企业用户通过卫星链路上传的数据，如企业办公网络中的文件传输、视频会议数据等，都会先到达POP节点。POP节点对这些数据进行初步处理，如检查数据的完整性和合法性。同时，POP节点也是数据分发的枢纽。它将从卫星接收到的数据按照目的地进行分发。对于要访问互联网的数据，POP节点会将其转发到地面的互联网骨干网。而对于企业内部网络之间的数据交换，POP节点会根据企业网络的拓扑结构将数据转发到相应的企业网络出口。例如，当一个企业内部的两个分支机构之间通过卫星互联网进行通信时，POP节点负责在这两个分支机构的网络出口之间转发数据。

3.8.2.1.1. 基于网络协议的漏洞挖掘

1）IP协议漏洞挖掘

在卫星互联网的POP节点中，IP地址欺骗是一个潜在的漏洞。由于卫星链路的特性，数据包的传输延迟和路径可能相对复杂。攻击者可能利用这一点，伪造源IP地址发送数据包到POP节点。例如，攻击者伪造一个合法企业的IP地址，向POP节点发送大量请求，试图绕过企业的网络安全防护措施。挖掘这种漏洞可以通过分析POP节点的入站流量，检查数据包的源IP地址与对应的MAC地址是否匹配，以及分析数据包的传输路径是否合理。例如，通过查看路由表中的源路由信息，如果发现源路由指向一个异常的网络段，而源IP地址却声称来自一个合法网络，这可能是IP地址欺骗的迹象。

IP分片攻击是针对IP协议的另一种潜在威胁。攻击者可以故意将正常的IP数据包分割成多个分片，然后在POP节点处进行恶意重组。例如，攻击者可能发送大量的IP分片，使POP节点的重组缓存溢出，导致节点崩溃或者出现异常行为。为了挖掘这种漏洞，需要对POP节点的IP分片处理机制进行深入研究，检查分片重组的缓存大小设置是否合理，以及对分片到达的顺序和时间间隔进行分析。例如，如果发现大量的IP分片在短时间内到达，且分片的标识和偏移量存在异常模式，这可能是IP分片攻击的迹象。

2）TCP协议漏洞挖掘

TCPSYN洪水攻击是一种常见的针对TCP协议的攻击方式，在POP节点也存在被攻击的风险。攻击者向POP节点发送大量的TCPSYN请求，但是不完成三次握手过程。由于POP节点需要为每个SYN请求分配一定的资源（如内存来存储连接状态等），大量的未完成握手请求会耗尽节点的资源。挖掘这种漏洞可以通过监测POP节点的TCP连接状态表，查看是否存在大量的SYN_RECV状态的连接，并且这些连接的源IP地址分布是否异常。例如，如果发现大量来自同一个网络段或者少量几个IP地址的SYN请求，且这些请求长时间处于SYN_RECV状态，这可能是TCPSYN洪水攻击的迹象。

在卫星互联网环境下，由于卫星链路的延迟和带宽特点，TCP序列号预测攻击可能有一定的隐蔽性。攻击者试图预测TCP连接中的序列号，从而伪造数据包插入到合法的TCP流中。例如，攻击者通过分析卫星链路的延迟特性和TCP流量模式，预测出下一个合法的TCP序列号，然后伪造包含恶意数据的数据包。要挖掘这种漏洞，需要对POP节点的TCP流量进行深度分析，检查TCP序列号的生成和使用模式，是否存在可预测的规律。例如，分析不同连接的TCP序列号的差值是否存在固定的模式，以及对连接的起始序列号进行统计分析，看是否存在异常的数值分布。

3.8.2.1.2. 应用层服务相关的漏洞挖掘

1）DNS服务漏洞挖掘

在POP节点中，DNS服务是非常重要的，它负责将域名转换为IP地址。DNS缓存投毒攻击是一种针对DNS服务的常见攻击方式。攻击者试图向POP节点的DNS服务器注入虚假的DNS记录，使得当用户请求某个域名时，DNS服务器返回攻击者指定的恶意IP地址。挖掘这种漏洞需要对DNS服务器的缓存更新机制进行监测，查看DNS缓存的更新来源是否合法，以及对DNS查询和响应进行分析。例如，检查是否存在来自异常源的DNS响应被接受并缓存的情况，或者分析DNS响应中的数据是否与已知的合法域名-IP地址映射存在冲突。

DNS放大攻击是利用DNS服务的特性进行的一种攻击。攻击者向POP节点的DNS服务器发送一个小的查询请求，利用DNS服务器的递归查询功能，使DNS服务器向多个目标发送大量的响应数据。攻击者通过伪造查询请求的源IP地址为POP节点的某个目标，从而使大量的响应数据涌向目标，造成目标的网络拥塞。挖掘DNS放大攻击漏洞需要对DNS服务器的查询和响应流量进行分析，查看是否存在异常的查询请求模式，如查询请求的源IP地址是否存在伪造的迹象，以及对DNS服务器的递归查询功能进行限制和监测。例如，检查是否存在对查询请求的源地址进行验证的机制，以及对递归查询的范围和频率是否有合理的限制。

2）Web服务漏洞挖掘

Web服务在互联网POP节点中广泛应用，用于提供各种网络服务，如用户认证、数据传输、远程管理等。POP节点的Web服务通常包括Web服务器软件、应用程序接口（API）、数据库管理系统等。Web服务的应用使得POP节点能够提供更加灵活和可扩展的服务，同时也为用户提供了便捷的管理和监控界面。由于Web服务在POP节点中的重要性，其安全性直接关系到整个卫星互联网地面网络的安全。Web服务漏洞可能导致数据泄露、服务中断、恶意攻击等严重后果。漏洞挖掘能够帮助发现和修复这些潜在的安全隐患，提高POP节点的安全性和可靠性，保护用户数据和网络服务的正常运行。

3.8.2.1.3. 安全策略与配置漏洞挖掘

1）访问控制策略漏洞挖掘

在POP节点的安全策略中，访问控制是重要的一环。如果访问控制策略设置过宽，可能会允许不必要的访问。例如，在某些POP节点中，可能存在对远程管理端口的访问控制过于宽松的情况，允许来自多个网络段甚至整个互联网的IP地址进行访问，这就给攻击者提供了可乘之机。挖掘这种漏洞需要对POP节点的访问控制列表（ACL）进行详细审查，检查每个ACL规则的源地址、目的地址、端口号和协议类型等参数。例如，查看是否存在允许任何源地址访问关键管理端口的规则，或者是否存在对特定服务的访问没有进行必要限制的情况。

身份认证是确保只有合法用户能够访问POP节点资源的关键措施。如果身份认证机制存在漏洞，如弱密码或者容易被绕过的认证方式，攻击者可能会获取非法访问权限。例如，在一些POP节点中，可能存在使用简单的用户名和密码组合进行认证的情况，或者存在认证过程中的逻辑漏洞，如可以通过暴力破解或者SQL注入等方式绕过认证。挖掘身份认证漏洞需要对POP节点的认证系统进行分析，检查认证算法的强度、密码的复杂度要求以及认证过程中的逻辑流程。例如，测试用户名和密码的可破解性，查看是否存在对特殊字符处理不当的情况，以及分析认证请求和响应之间的交互是否存在可利用的漏洞。

2) 路由配置漏洞挖掘

在POP节点中，静态路由是网络路由的重要组成部分。如果静态路由设置错误，可能会导致网络不通或者形成路由环路。例如，在设置从POP节点到某个企业网络的静态路由时，如果目的网络地址或下一跳地址设置错误，数据包将无法正确到达目的地，或者可能在网络中不断循环。挖掘这种漏洞需要对POP节点的静态路由表进行详细检查，查看每个静态路由条目的目的网络、掩码、下一跳地址等参数是否正确。例如，通过对比实际的网络拓扑结构和静态路由表中的设置，检查是否存在不匹配的情况，以及对静态路由条目的优先级设置是否合理。

POP节点中使用的动态路由协议（如OSPF、BGP等）如果配置不当，可能会导致路由不稳定或者安全问题。例如，在OSPF配置中，如果区域划分不合理或者认证设置不当，可能会导致路由信息泄露或者路由表被篡改。挖掘动态路由协议配置漏洞需要对路由协议的配置文件进行深入分析，检查协议的参数设置，如OSPF的区域类型、认证方式、路由器ID等参数是否符合安全和性能要求。同时，对路由协议的运行状态进行监测，查看是否存在频繁的路由更新、路由振荡等异常情况。

3.8.2.2. 地面信关站

地面信关站是卫星互联网地面网络中的关键设施，其结构复杂且包含多个功能模块。从硬件方面来看，它包含天线系统、射频（RF）收发模块、基带处理单元等。天线系统负责接收和发送卫星信号，其类型多样，如抛物面天线等，其性能直接影响信号的接收和发送质量。射频收发模块用于在射频频段对信号进行处理，包括信号的调制、解调、放大等操作。基带处理单元则承担着对数字信号的处理任务，如编码、解码、多址接入处理等。

在软件层面，地面信关站运行着复杂的操作系统和各种通信协议栈。操作系统负责管理信关站的硬件资源，协调各个功能模块之间的工作。通信协议栈则确保信关站能够与卫星、地面终端以及其他网络设备进行有效的通信。例如，它需要遵循卫星通信特定的协议，如DVB-S2（数字视频广播-卫星第二代）协议等用于卫星信号的传输，同时也需要遵循地面网络的协议，如TCP/IP协议用于与地面网络的交互。

地面信关站的主要功能之一是实现卫星链路与地面网络的连接转换。它接收来自卫星的信号，将卫星信号转换为适合地面网络传输的格式，然后将数据转发到地面网络中的目的地，如互联网服务提供商（ISP）的网络或者企业网络等。反之，它也接收来自地面网络的上行数据，将其转换为卫星通信格式后发送到卫星上。

此外，地面信关站还承担着信号的处理与优化功能。在接收端，它需要对微弱的卫星信号进行放大、滤波等处理，以提高信号的质量。同时，它还需要进行多址接入处理，区分不同用户或终端的信号，确保数据的正确接收和分发。在发送端，它要对信号进行编码、调制等操作，以提高信号在卫星链路中的传输效率和可靠性。

3.8.2.2.1. 基于网络层的漏洞挖掘

1) IP地址欺骗

在地面信关站与地面网络的交互中，IP地址欺骗是一种潜在的威胁。攻击者可能伪造IP地址向信关站发送数据包，试图绕过信关站的安全防护或者进行恶意攻击。挖掘IP地址欺骗漏洞需要对信关站的入站数据包进行IP地址检查，可以采用源IP地址验证技术，如反向路径转发（RPF）检查。通过查看数据包的源IP地址对应的路由路径是否与实际的网络拓扑相符，如果发现存在不相符的情况，就可能是IP地址欺骗行为。同时，可以对频繁出现异常IP地址的源进行封锁或进一步调查。

2) IP地址分配漏洞

面信关站负责对地面终端进行IP地址分配，IP地址分配过程可能存在漏洞。例如，可能存在IP地址分配冲突的情况，导致网络通信混乱。或者在动态IP地址分配过程中，如果没有对终端的身份进行有效的验证，可能会导致非法终端获取合法的IP地址。挖掘IP地址分配漏洞需要对信关站的IP地址分配机制进行审查，检查IP地址分配表是否存在重复分配的情况，对于动态IP地址分配，需要检查是否有完善的身份验证和地址回收机制。可以通过模拟多个终端请求IP地址的场景来测试IP地址分配机制的有效性。

3.8.2.2.2. 基于应用层的漏洞挖掘

1) DNS服务漏洞挖掘

地面信关站如果提供DNS服务或者依赖DNS服务进行域名解析，就可能面临DNS缓存投毒的风险。攻击者可能向信关站的DNS服务器发送伪造的DNS响应，使信关站将恶意的IP地址与合法的域名关联起来。挖掘DNS缓存投毒漏洞需要对DNS服务器的缓存更新机制进行严格监控，检查DNS服务器是否对接收的DNS响应进行来源验证，是否存在接受未经验证的DNS响应并将其缓存的情况。可以通过设置DNS响应的白名单或者采用DNSSEC（DNS安全扩展）技术来防范DNS缓存投毒攻击。

DNS放大攻击是利用DNS服务的特性进行的一种攻击。攻击者向信关站的DNS服务器发送小的查询请求，利用DNS服务器的递归查询功能，使DNS服务器向多个目标发送大量的响应数据，从而导致网络拥塞。挖掘DNS放大攻击漏洞需要对DNS服务器的查询和响应流量进行分析，查看是否存在异常的查询请求模式，如查询请求的源IP地址是否存在伪造的迹象。同时，需要对DNS服务器的递归查询功能进行限制，如设置查询的最大递归深度、限制查询的源地址范围等。

2）Web服务漏洞挖掘

如果地面信关站提供Web服务，如用于管理界面或用户服务，可能会受到SQL注入攻击。攻击者通过在Web表单或URL中注入恶意的SQL语句，试图获取信关站数据库中的敏感信息或者执行恶意操作。

在地面信关站的Web服务中，跨站脚本攻击也是一个潜在的风险。攻击者可以将恶意脚本注入到Web页面中，当用户访问该页面时，恶意脚本会在用户的浏览器中执行，可能会窃取用户的会话信息或者执行其他恶意操作。

3.8.2.3. 地面终端

卫星互联网地面终端的硬件结构包含多个关键组件。天线是地面终端的重要组成部分，其类型和性能对信号的接收和发送有着直接影响。例如，小型化的抛物面天线或相控阵天线被广泛应用于地面终端。抛物面天线具有较高的增益，但体积相对较大；相控阵天线则可以通过电子控制实现波束的灵活指向，并且在体积和重量方面有一定优势。

射频（RF）模块负责对射频信号进行处理，包括信号的放大、滤波、变频等操作。它将天线接收到的微弱卫星信号进行初步处理，将其转换为适合后续处理的中频信号。基带处理单元则主要进行数字信号的处理，如解调解码、信道编码等操作。此外，地面终端还包含电源管理模块，为各个组件提供稳定的电力供应，由于卫星互联网可能在不同的环境下使用，电源管理模块需要具备一定的适应性，如支持电池供电或者从多种电源接口获取电力。

处理器和存储器组件在地面终端中负责运行操作系统和相关应用程序，同时存储用户数据和系统配置信息。处理器的性能决定了地面终端对数据处理的速度和能力，而存储器的容量则限制了可以存储的数据量和可运行的程序规模。

地面终端运行着操作系统，如定制的Linux系统或专门开发的嵌入式操作系统。操作系统负责管理硬件资源，包括对天线、射频模块、基带处理单元等硬件的驱动和控制。同时，它提供了一个软件运行的平台，支持各种应用程序的运行。

通信协议栈是地面终端软件的核心部分。它遵循卫星通信的相关协议，如DVB-S2协议等用于接收卫星信号，以及在与地面网络交互时遵循TCP/IP协议。通信协议栈确保地面终端能够正确地接收、发送和处理数据，包括对数据的封装、解封装、路由等操作。地面终端还可能具备用户界面软件，用于用户与终端的交互。例如，通过图形界面或命令行界面，用户可以进行网络连接的配置、查看信号强度、管理用户账户等操作。另外，安全相关的软件功能也是必不可少的，如加密解密算法的实现，以确保数据在传输和存储过程中的安全性。

3.8.2.3.1. 基于硬件层面的漏洞挖掘

1）天线相关漏洞挖掘

地面终端的天线需要精确指向卫星，以保证良好的信号接收和发送。然而，由于多种因素，天线的指向精度可能会受到影响。例如，在安装过程中，如果没有精确校准，或者受到外界环境的干扰（如风、震动等），天线的指向可能会发生偏差。挖掘这种漏洞可以通过检测天线的接收信号强度指示（RSSI）。如果RSSI值低于正常水平，且在排除卫星信号源功率变化等因素后，很可能是天线指向精度出现问题。另外，可以利用卫星定位和地面终端的地理位置信息，结合天线的设计指向角度，计算出理论的天线指向，与实际指向进行对比。

天线的性能可能随着时间的推移而退化，这可能是由于材料老化、环境腐蚀等原因造成的。例如，天线表面的涂层脱落可能会影响其反射性能，从而降低天线增益。为了挖掘天线性能退化的漏洞，需要定期对天线的增益、方向图等性能指标进行测试。可以使用专业的天线测试设备，如矢量网络分析仪，将测试结果与天线的初始性能指标进行对比。如果发现增益明显下降或者方向图出现异常变化，就需要进一步检查天线的物理结构和材料状况。

2）射频模块漏洞挖掘

射频模块容易受到外界射频干扰的影响。例如，附近的其他无线通信设备、工业设备产生的电磁干扰等都可能干扰射频模块的正常工作。这种干扰可能导致信号的误码率增加、接收灵敏度下降等问题。挖掘射频干扰敏感性漏洞可以通过在射频模块附近设置射频监测设备，对周围的射频环境进行监测。分析监测到的射频信号的频率、功率和频谱特征，查找是否存在与射频模块工作频率相近的干扰信号。同时，可以通过在实验室环境下，人为施加不同类型和强度的干扰信号，观察射频模块的工作状态，如信号的接收和处理能力是否受到影响。

射频模块中的组件，如放大器、滤波器、混频器等，可能会出现故障。例如，放大器的功率输出不稳定可能导致信号强度波动，滤波器的通带特性改变可能会使有用信号被衰减而干扰信号被放大。挖掘射频组件故障漏洞需要对射频模块的关键组件进行性能监测。例如，监测放大器的输入和输出功率、电流、温度等参数。如果发现输出功率与输入功率的比值（放大倍数）不稳定，或者功率输出波动较大且伴有电流或温度异常变化，就可能是放大器出现故障。对于滤波器，可以通过扫频测试其通带和阻带特性，检查是否与设计指标相符。

3）终端设备问题

以国外VSAT市场骨干供应商为主要研究对象，通过对主流设备长期跟踪、解析、测试、试验后认为：这些供应商在关键设备、枢纽部件上有意无意、或多或少的预制后门，留有漏洞。以某产品为例的分析如下：

第一、采用分层密钥管理体系结构。顶层密钥在国外厂商手中，对其设备承载的卫星通信网络可迅速还原加密业务。

第二、使用的加密算法含有较为脆弱的过时算法，以目前业内非专业网络密码破译水平和简单计算工具即可达成破译。高加密强度级别产品只对本国及盟国发售。

第三、通过对设备固件进行提取分析发现，广泛存在厂商预置的账号，用于远程登录和管理控制。通常卫星网络入侵，以及Viasat卫星网络攻击事件就是采取此类方法，存在重大安全隐患。

3.8.2.3.2. 基于软件层面的漏洞挖掘

1）操作系统漏洞挖掘

地面终端所运行的操作系统内核可能存在漏洞。例如，在Linux内核中，可能存在缓冲区溢出漏洞、权限提升漏洞等。这些漏洞可能被攻击者利用，从而获得对终端系统的更高权限或者执行恶意代码。挖掘内核漏洞需要对操作系统内核的版本进行跟踪。与操作系统厂商发布的漏洞公告进行比对，同时可以使用专门的内核漏洞扫描工具进行检测。例如，一些开源的漏洞扫描工具可以对Linux内核进行全面扫描，查找是否存在已知的漏洞。此外，对内核的配置文件进行审查，检查是否存在不安全的配置选项，如开启了不必要的服务或者权限。

操作系统的驱动程序用于控制硬件设备，如天线、射频模块的驱动程序等。如果驱动程序存在漏洞，可能会导致硬件设备无法正常工作或者被恶意控制。例如，天线驱动程序中的漏洞可能导致天线无法正确指向卫星，或者被攻击者利用改变天线的指向。挖掘驱动程序漏洞需要对驱动程序的源代码（如果可获取）进行审查。检查驱动程序中的函数调用是否存在安全隐患，如对输入参数的验证是否充分、内存管理是否安全等。同时，可以通过在不同的硬件环境和使用场景下测试驱动程序的稳定性和安全性，观察是否会出现异常的硬件操作或系统崩溃现象。

2）通信协议栈漏洞挖掘

地面终端遵循的卫星通信协议可能存在漏洞。例如，在协议的帧结构、编码方式等方面可能存在缺陷，被攻击者利用进行信号干扰或数据篡改。挖掘卫星通信协议漏洞需要对协议的标准文档进行深入研究，分析协议的各个环节。通过模拟攻击场景，如发送不符合协议规范的数据包，观察终端的反应。如果终端出现异常的接收或处理行为，如误码率异常升高或者无法正确解析数据包，就可能是协议存在漏洞。同时，可以参考相关的学术研究和行业安全报告，了解是否有其他研究人员发现了类似协议的漏洞。

在与地面网络交互时，地面终端遵循的TCP/IP协议也可能存在漏洞。例如，TCP协议中的SYN洪水攻击、IP协议中的地址欺骗等问题都可能影响地面终端与地面网络的正常通信。挖掘地面网络协议漏洞可以采用与挖掘卫星通信协议漏洞类似的方法。对TCP/IP协议的各个子协议进行详细分析，通过网络监测工具观察终端在网络中的通信行为。例如，监测TCP连接的状态，查看是否存在大量的SYN_RECV状态的连接，这可能是SYN洪水攻击的迹象。对于IP地址欺骗，可以检查终端对入站数据包的源IP地址验证机制是否完善。

3.8.2.3.3. 基于网络连接的漏洞挖掘

1）卫星链路连接漏洞挖掘

在地面终端与卫星建立链路时，可能会遇到各种问题。例如，由于卫星轨道位置的变化或者地面终端的位置移动，可能导致链路建立失败。此外，在链路维持过程中，如果信号受到遮挡（如建筑物、树木等）或者受到干扰，链路可能会中断。挖掘链路建立与维持问题的漏洞需要对链路建立和维持的过程进行详细监测。记录链路建立过程中的各个参数，如信号强度、频率锁定情况等。如果链路建立失败，可以分析这些参数是否在正常范围内。对于链路维持，可以设置信号强度的阈值，当信号强度低于阈值时，判断链路可能出现问题。同时，可以利用卫星的轨道数据和地面终端的移动轨迹（如果适用）预测可能出现链路问题的情况。

卫星的资源是有限的，如带宽、时隙等。地面终端在使用卫星资源时，可能会面临资源分配不合理或者资源竞争的问题。例如，如果多个地面终端在同一区域同时请求大量的卫星带宽，可能会导致部分终端无法获得足够的带宽，从而影响通信质量。挖掘卫星资源分配问题的漏洞需要对卫星资源分配的机制进行研究。了解卫星是如何根据地面终端的需求分配资源的，如是否采用了公平的分配算法。通过监测多个地面终端的资源使用情况，查看是否存在资源分配不均衡的现象。例如，可以统计不同地面终端的带宽使用量，分析是否存在部分终端长期占用大量带宽而其他终端带宽不足的情况。

2）地面网络连接漏洞挖掘

地面终端在接入地面网络时，可能存在网络接入漏洞。例如，如果采用Wi-Fi接入地面网络，Wi-Fi的安全协议（如WPA、WPA2等）可能存在漏洞。攻击者可能利用这些漏洞破解Wi-Fi密码，从而非法接入与地面终端相连的网络。挖掘网络接入漏洞需要对地面终端所采用的网络接入方式进行详细分析。对于Wi-Fi接入，检查所使用的安全协议版本，是否存在已知的漏洞。可以使用Wi-Fi漏洞扫描工具对终端的Wi-Fi连接进行检测，查看是否存在弱密码、加密方式可破解等问题。对于其他网络接入方式，如以太网接入，需要检查网络接口的访问控制是否严格，是否存在未经授权的设备可以接入的情况。

地面终端在地面网络中的路由选择也可能存在漏洞。例如，如果地面网络采用动态路由协议（如OSPF、RIP等），地面终端可能会受到路由欺骗攻击。攻击者可能伪造路由信息，使地面终端将数据包发送到错误的目的地。挖掘网络路由漏洞需要对地面终端所在的地面网络的路由协议进行研究。检查地面终端是否对路由信息进行了有效的验证，如是否检查路由通告的来源、路由的合法性等。可以通过模拟路由欺骗攻击场景，观察地面终端的反应。如果地面终端接受了伪造的路由信息并改变了数据包的发送路径，就说明存在路由漏洞。

3.8.3. 卫星互联网通信网络的漏洞挖掘

卫星互联网通信旨在通过卫星星座实现全球范围内的信息传输与交互。空口信道侧是卫星与地面终端之间直接进行信号传输，涵盖了从信号的发射、传播到接收的全过程，这一过程涉及多种复杂的技术和协议。

3.8.3.1. 基于信号发射的漏洞挖掘与分析

(一)信号发射功率相关漏洞

1) 功率控制不准确

在卫星发射信号时,功率控制是一个关键环节。如果功率控制算法存在缺陷,例如没有充分考虑到卫星与地面终端之间距离的动态变化、大气衰减的不确定性等因素,就可能导致发射功率不准确。

一些卫星可能采用固定功率发射模式,没有根据实际通信情况进行自适应调整。当卫星与地面终端距离较近时,过高的发射功率可能会造成对其他卫星或地面系统的干扰;而当距离较远时,过低的发射功率则可能使地面终端无法接收到足够强度的信号。

对于其他卫星或地面系统的干扰可能会引发一系列连锁反应。例如,干扰可能影响地面无线电通信系统的正常运行,导致地面通信基站的误码率升高,影响手机通信、广播电视等业务。对地面终端而言,信号接收不足会导致通信中断或严重的误码问题,影响数据传输、语音通话和视频流等业务的质量。

2) 功率放大器故障模式下的漏洞

卫星上的功率放大器是确保信号足够强度发射的关键设备。如果功率放大器出现故障,如出现增益下降、线性度变差等情况,可能会导致发射信号功率异常。

功率放大器的故障可能是由于长时间运行导致的器件老化、太空环境中的辐射损伤或者供电系统不稳定等原因引起的。在故障情况下,卫星可能无法按照正常功率发射信号,而系统可能缺乏有效的故障检测和应对机制。

当功率放大器增益下降时,发射信号功率降低,地面终端接收到的信号变弱,增加误码率,甚至可能无法建立通信链路。线性度变差可能会引入信号失真,影响信号的调制和解调准确性,导致通信质量下降,在数据传输业务中可能会出现数据丢失或错误的情况。

（二）发射信号调制相关漏洞

1）调制方式选择漏洞

在卫星互联网通信中，调制方式的选择需要综合考虑多种因素，如传输速率、抗干扰能力、频谱利用率等。如果选择的调制方式不适合特定的通信场景，就会存在漏洞。例如，在高噪声和干扰环境下，选择了相对简单的调制方式（如BPSK），而没有采用抗干扰能力更强的高阶调制方式（如8PSK或16QAM）。或者在频谱资源紧张的情况下，没有选择频谱利用率高的调制方式。

不恰当的调制方式会导致在特定环境下通信性能下降。在高噪声环境下，简单调制方式的误码率会显著增加，影响数据传输的准确性。对于频谱利用率低的调制方式，会浪费宝贵的频谱资源，限制卫星互联网能够支持的用户数量和业务容量。

2）调制参数设置漏洞

调制过程中的参数设置对于信号的正确传输至关重要。例如，在QPSK调制中，相位偏移量的设置如果不准确，会导致接收端无法正确解调信号。一些卫星通信网络可能在调制参数设置方面缺乏灵活性，不能根据不同的通信条件（如不同的地面终端类型、不同的传输距离等）进行自适应调整。调制参数不准确会直接导致信号解调失败，使通信中断。缺乏自适应调整能力会导致在不同通信条件下通信性能不稳定，例如在长距离传输时，固定的调制参数可能无法保证信号质量，导致误码率升高，影响数据传输的可靠性。

3.8.3.2. 空口传播过程中的漏洞挖掘与分析

在卫星通信的空口信道中，信号可能通过多条不同的路径到达地面接收端，这就是多径传播现象。多径传播可能是由于地面反射、大气折射等原因造成的。如果卫星通信网络没有有效的多径抑制技术，如采用合适的分集接收技术（空间分集、极化分集等）或多径均衡技术，就会受到多径效应的严重影响。

多径传播会导致信号的衰落和时延扩展。信号衰落会使接收端接收到的信号强度波动，增加误码率。时延扩展会使信号的不同路径分量在时间上散开，导致码间干扰，影响信号的正确解调，在高速数据传输业务中可能会造成严重的性能下降。

3.8.3.3. 多址接入技术相关的漏洞挖掘与分析

（一）时分多址（TDMA）漏洞

1）时隙分配与同步漏洞

在TDMA系统中，时隙分配是关键。如果时隙分配不合理，例如没有根据不同用户的业务需求和优先级进行分配，可能会导致一些用户的业务延迟或阻塞。

TDMA系统对时间同步要求极高，地面终端与卫星之间需要精确的时间同步。如果时间同步出现偏差，可能会导致时隙冲突，即不同终端在同一时隙发送或接收信号，从而造成信号碰撞和通信中断。

时隙分配不合理会影响用户的服务质量，对于实时性要求高的业务（如语音通话、视频会议）会造成通话卡顿、图像不流畅等问题。时隙冲突会导致通信无法正常进行，需要重新进行同步和时隙分配，这会增加通信的延迟和开销。

2）动态时隙调整漏洞

TDMA系统需要能够根据用户业务量的变化进行动态时隙调整。如果缺乏有效的动态时隙调整机制，当用户业务量突然增加或减少时，就无法及时调整时隙分配，导致资源浪费或用户业务无法满足需求。

在业务量增加时，无法及时分配更多时隙会导致部分用户的业务无法正常进行，如数据传输速度慢或无法接入。在业务量减少时，不能及时回收多余时隙会浪费卫星通信资源，降低系统的整体效率。

（二）频分多址（FDMA）漏洞

1）频段划分与保护漏洞

FDMA系统将频段划分为多个子频段供不同用户使用。如果频段划分不合理，例如子频段宽度设置不当，可能会导致频谱利用率低下。

相邻子频段之间需要设置保护带以避免干扰，但如果保护带设置过窄，就会出现频率泄漏现象，即一个子频段的信号会泄漏到相邻子频段，造成相邻子频段的干扰。

频谱利用率低下会限制卫星互联网通信能够支持的用户数量和业务容量。相邻子频段的干扰会增加误码率，影响通信质量，导致用户体验下降。

2）频率管理漏洞

在FDMA系统中，频率管理至关重要。如果没有有效的频率管理机制，可能会出现频率分配冲突的情况，即多个用户被分配到相同的频率资源。

此外，随着卫星通信业务的发展，新用户的加入可能需要重新分配频率资源，如果频率管理缺乏灵活性，就无法满足新用户的需求。

频率分配冲突会导致通信中断或严重的干扰问题。无法满足新用户需求会限制卫星互联网通信的发展，使其无法适应不断增长的市场需求。

（三）码分多址（CDMA）漏洞

1）扩频码特性漏洞

CDMA系统中，每个用户使用不同的扩频码进行信号扩频。如果扩频码的自相关性和互相关性特性不理想，例如自相关性不够强、互相关性过高，就会导致码间干扰。

扩频码的选择和分配如果缺乏有效的管理机制，可能会出现扩频码重复分配或分配不合理的情况，影响不同用户之间的信号区分。

码间干扰会使接收端无法正确区分不同用户的信号，增加误码率，影响通信质量。扩频码分配不合理会导致用户之间的干扰，降低系统的容量和性能。

2）功率控制漏洞

CDMA系统中的功率控制非常复杂。如果功率控制算法不完善，例如不能根据用户与卫星的距离、信道状况等因素进行自适应功率控制，就会出现功率不平衡的情况。

当某个用户的发射功率过高时，会对其他用户造成多址干扰，降低整个系统的性能；而功率过低则可能导致该用户的信号无法被正确接收。

多址干扰会影响其他用户的通信质量，使整个系统的容量下降，无法满足更多用户的需求。功率过低会使通信中断或误码率升高，影响用户的业务体验。

3.8.3.4. 卫星轨道与覆盖相关的漏洞挖掘与分析

(一)卫星轨道参数与通信漏洞

1) 轨道精度影响

卫星的轨道参数(如轨道高度、轨道倾角、偏心率等)对通信有重要影响。如果轨道精度控制不佳,卫星的实际轨道与设计轨道存在较大偏差,可能会导致卫星覆盖范围变化。

例如,轨道高度降低可能会使卫星的覆盖范围缩小,影响地面某些区域的通信服务。而轨道高度升高可能会导致信号传播时延增加,对实时性业务产生不利影响。

卫星覆盖范围缩小会使部分地面区域失去卫星互联网通信服务,影响当地用户的正常通信需求。信号传播时延增加会降低通信效率。

2) 轨道摄动影响

卫星在运行过程中会受到多种摄动因素的影响,如地球引力场不均匀性、日月引力、大气阻力等。如果没有充分考虑到这些摄动因素对轨道的影响,就可能导致卫星轨道的不稳定。

轨道不稳定会使卫星的位置难以准确预测,影响卫星与地面终端之间的通信链路建立和保持。

卫星位置难以预测会导致地面终端无法准确指向卫星进行通信,增加通信建立的难度。在通信过程中,可能会因为卫星位置的突然变化而导致通信中断,影响业务的连续性。

(二)卫星覆盖漏洞

1) 覆盖盲区漏洞

由于卫星星座布局、地球曲率、地形遮挡等因素,可能会存在卫星覆盖盲区。如果没有合理规划卫星星座或者采用有效的技术手段来弥补覆盖盲区,地面的某些区域将无法获得卫星互联网通信服务。

例如,在山区、峡谷等地形复杂的地区,卫星信号可能被山脉遮挡,形成覆盖盲区。

覆盖盲区会使这些区域的用户无法使用卫星互联网通信,限制了卫星互联网的服务范围,影响了通信的普遍性和公平性。

2）覆盖重叠区域漏洞

在卫星覆盖区域存在重叠的情况下，如果没有合理的资源分配和干扰协调机制，可能会导致在重叠区域内信号干扰增加。

例如，多个卫星在重叠区域同时发射信号，如果频率、功率等资源没有协调好，会导致信号碰撞和干扰。

信号干扰增加会提高误码率，降低通信质量，影响重叠区域内用户的通信体验。在数据传输业务中，可能会出现数据丢失或错误的情况。

参考文献与数据来源

[1] Viasat卫星通信网络攻击案例警示：黑客会如何攻击脆弱的卫星网络?-安全内参|决策者的网络安全知识库，URL:https://www.secrss.com/articles/40946，2022年。

[2] 刘卫：《太空碰撞，危险如何规避?》URL:https://m.gmw.cn/baijia/2022-01/20/35459711.html, 2022年。

[3]史军良、周宏新：《卫星通信中的常见干扰分类及处理方法》，URL: https://www.c114.com.cn/tech/164/a359449.html。

[4] 中信卫星：《浅谈OneWeb星座》，URL：https://www.citicsat.com/Info_News/14/193。

[5] 星座卫星数量与分布情况：URL https://satellitemap.space/

[6] 卫星互联网测绘数据：URL https://www.daydaymap.com/home

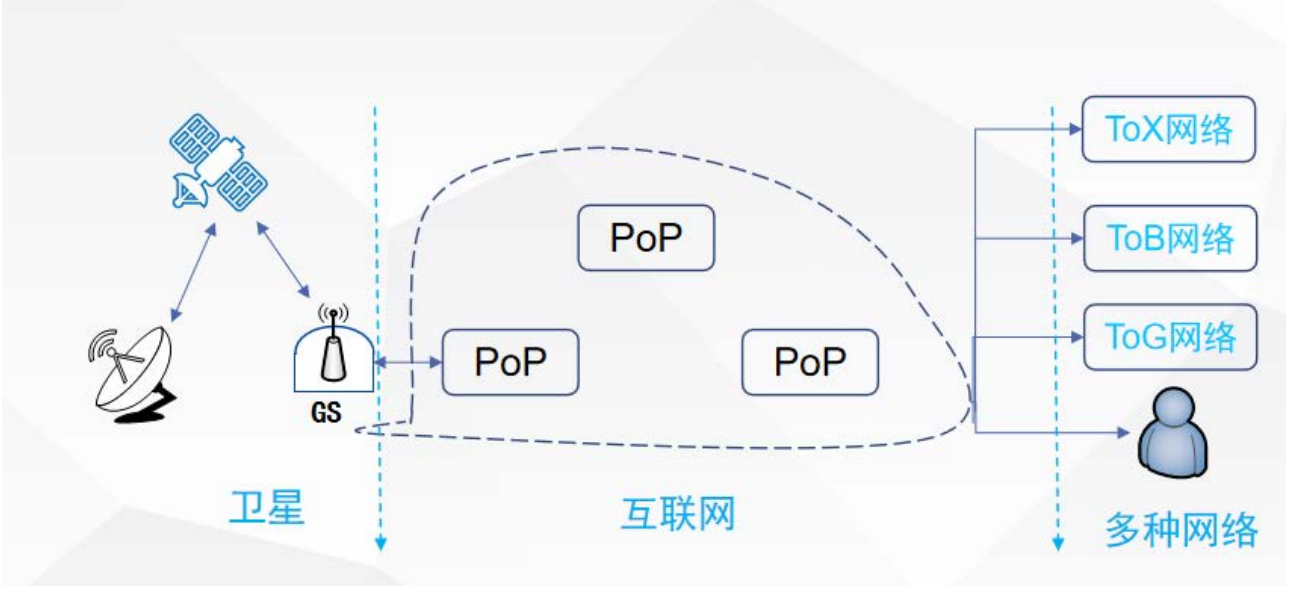
附件1

针对卫星互联网的观点

盛邦安全及联合团队通过对典型低轨星座网络测绘，自治域组成分析，全球信关站布局分析，终端剖析，服务网元分析，路由及时延分析，同时对比传统卫星网络，形成卫星互联网基本观点如下：

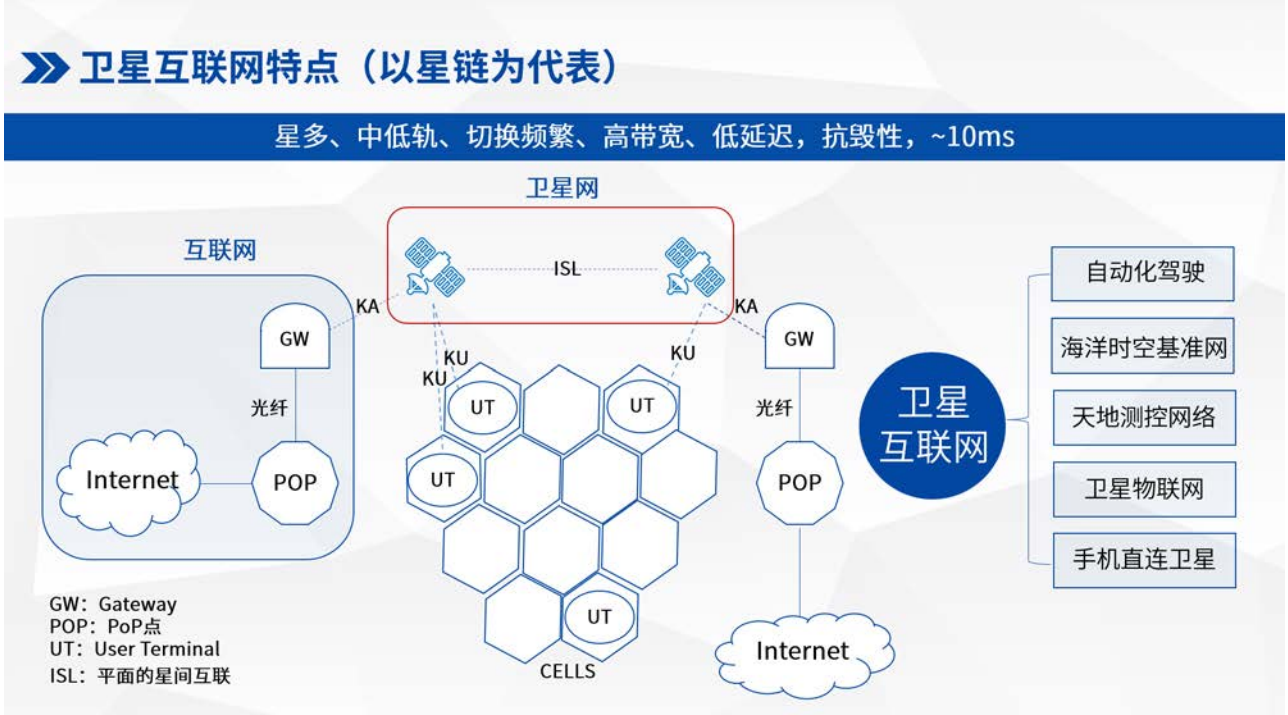
一、卫星互联网不是卫星网的升级改造，而是重构

卫星互联网的每个网络节点，包括星载节点，都是按照尽力服务的互联网理念进行建设，由于降低了可靠性要求和服务质量要求，可以采用地面成熟的技术和器件设计卫星载荷，大幅度降低了单个星载节点的成本和能力要求，大幅降低了单个节点的复杂度；同时，使用系统工程的建设思路，采用星座建设与互联网相互融合，提高了整个系统的可用性、可靠性和健壮性。



卫星互联网接入服务

传统卫星通信网



卫星互联网的组网

RTT看卫星 VS 卫星互联网

星链的RTT高于其他地面网络，但是比其他GEO SatCom好很多

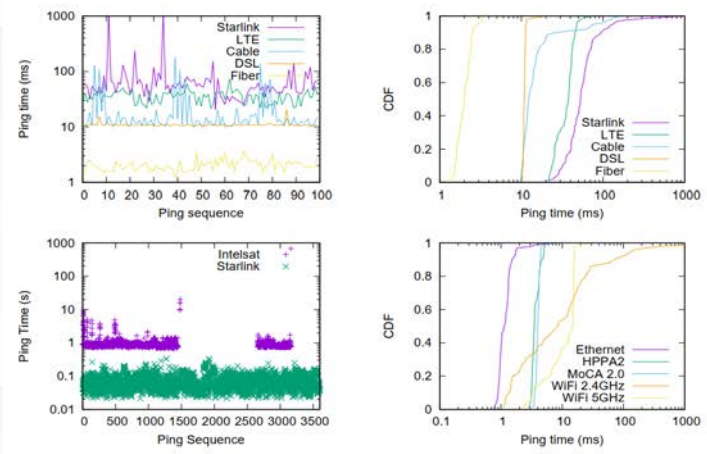


Fig. 3. Starlink access performance compared with other technologies.

卫星互联网与卫星通信网RTT对比

市场变化（截至2024H1）

	重点/优先	客户群 (YE 2022)	客户群 (YE 2024)
住宅	✓	~1m 订阅者	~4m 订阅者
商业	✓	~155K 商业	320K+ 商业
车载	✓	~110K 用户	~230K 用户
移动性 （海事）	✓	~500 船只	~3,500 船只
航空	✓	~50 飞机	~160 飞机

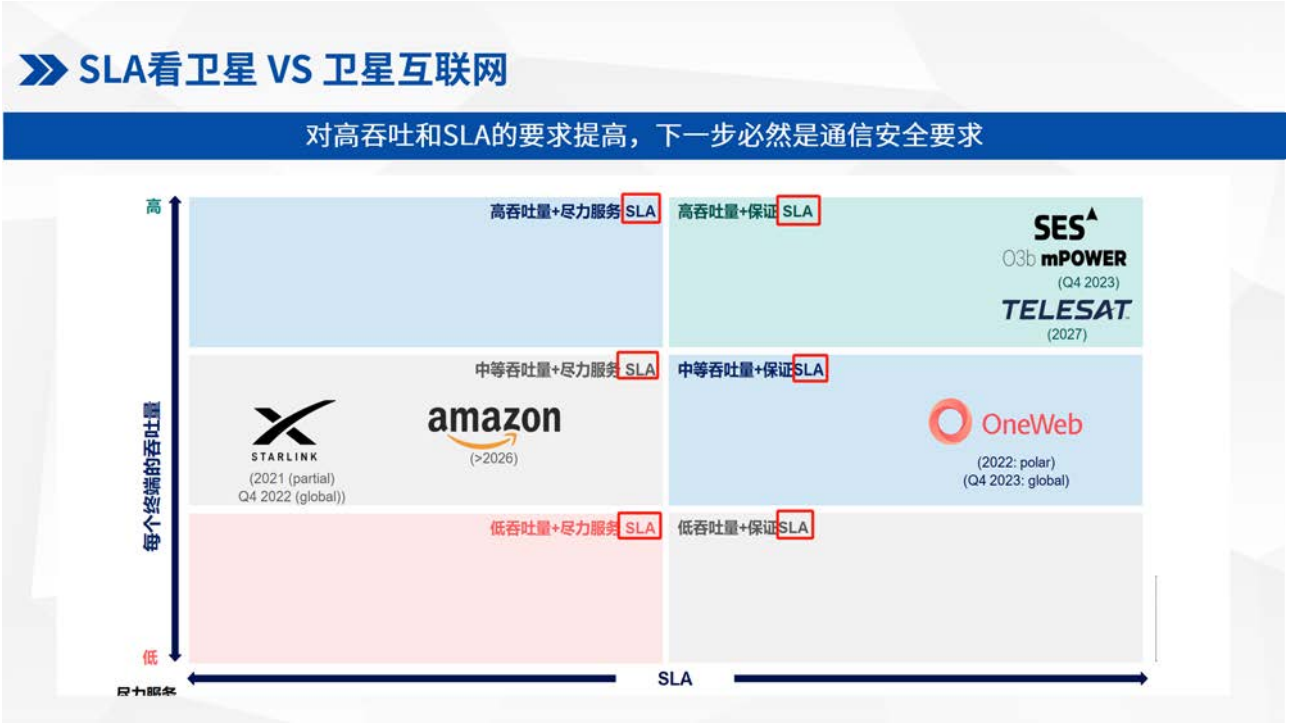
MARKET FOCUS/PRIORITY: ✓ Primary ✓ Secondary

传统卫星网络厂商十多年积累用户数：

Hughesnet：
~ 150万订阅用户

Viasat：
~ 70万订阅用户

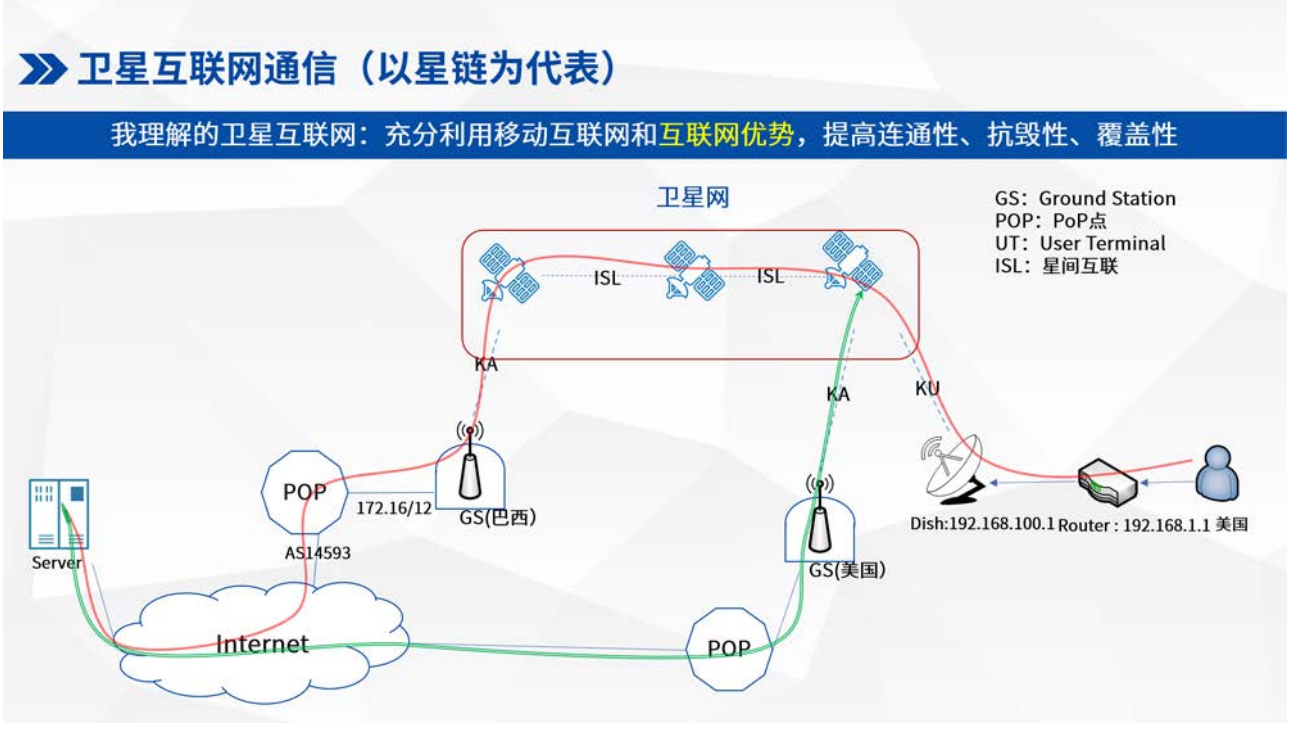
用户对比


SLA看卫星 VS 卫星互联网
对高吞吐和SLA的要求提高，下一步必然是通信安全要求
高
每个终端的吞吐量
低
高吞吐量+尽力服务 SLA
高吞吐量+保证 SLA
SES
O3b mPOWER
(Q4 2023)
TELESAT
(2027)
中等吞吐量+尽力服务 SLA
中等吞吐量+保证SLA
STARLINK
(2021 (partial)
Q4 2022 (global))
amazon
(>2026)
OneWeb
(2022: polar)
(Q4 2023: global)
低吞吐量+尽力服务 SLA
低吞吐量+保证SLA
SLA

服务质量对比

二、卫星网最后一公里是网络，卫星互联网最短的一公里是卫星

地面网络是卫星互联网业务传输的骨干，下图绿色部分是实际业务数据的传输路径。

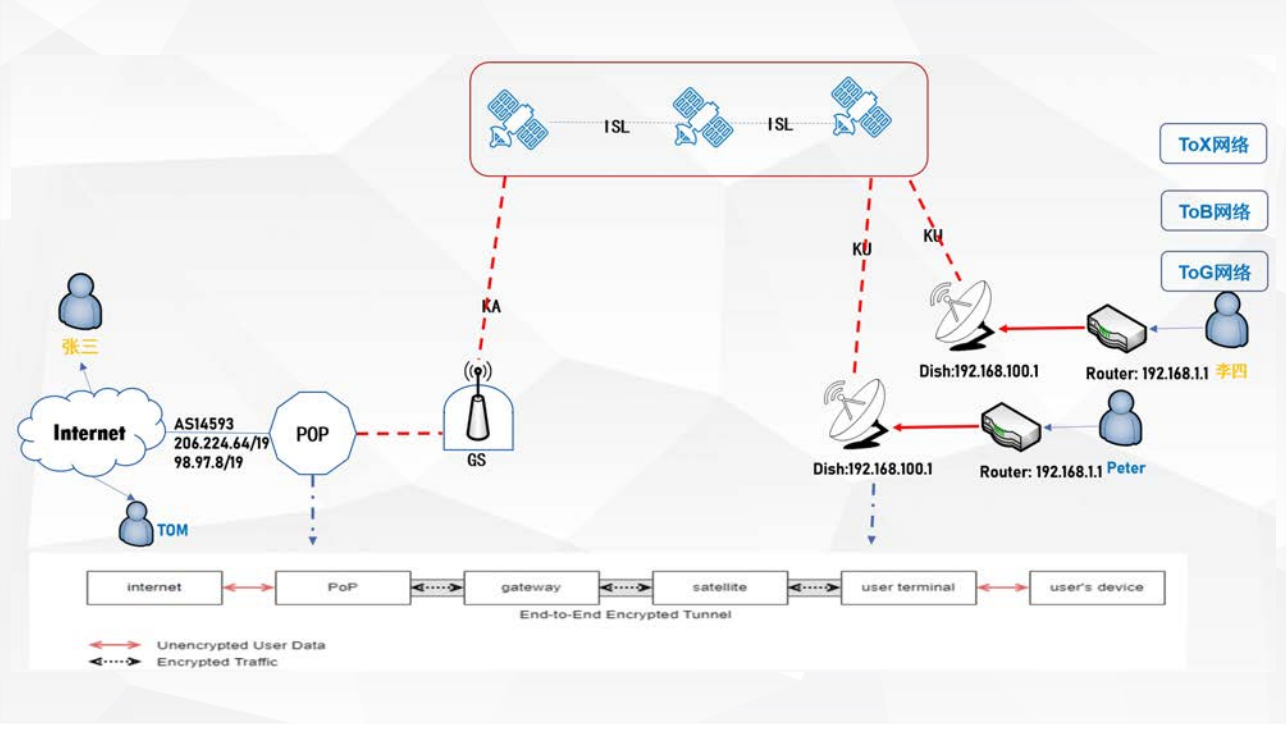


卫星互联网的数据路径

与传统卫星网理念相悖的是：星链低轨星座是以地面网络为主要通信链路。绝大多数的业务流量是通过地面网络进行路由和中转，只有少部分的业务流量是通过星间链传递的。卫星互联网把卫星作为接入节点或信号延伸的通道，将通信数据尽快落地，通过地面网络来服务更多的用户，实现更大范围的业务覆盖。

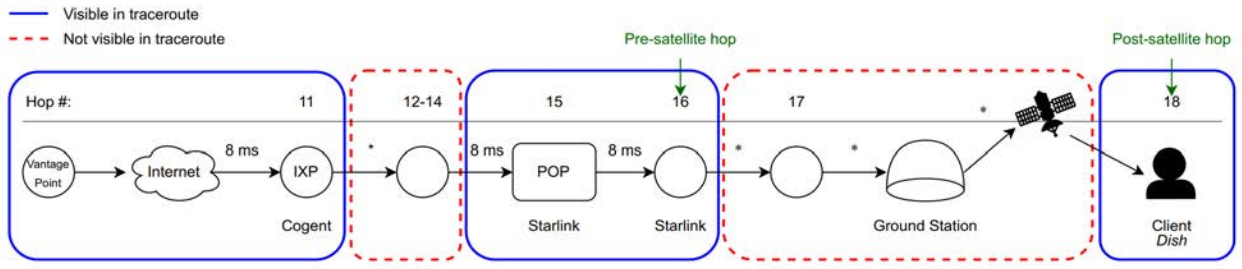
三、通过密码定义卫星互联网的用户和边界，保障数据安全和网络安全

简化网络设计，采用一张网策略，通过密码定义网络和用户边界，保障了运控安全、测控安全、运维安全、传输安全和数据安全，这个不同于传统互联网的安全体系。



网络隔离

从安全域看卫星互联网的组网结构



组网结构

由于卫星通信的开放性和暴露性，传统的互联网安全手段，包括安全访问列表、网段逻辑隔离等技术不能解决用户网络隔离、管用分离等安全需求。使用一张网，通过采用密码定义网络边界和用户边界，低轨星座既能够为不同用户提供隔离的网络服务，通过密码定义用户边界；通过构建专用的运控VPN网络，同时也能管控到星座的每一个节点，包括星载不同载荷，终端每一个服务网元，甚至信关站的物联网设备，诸如空调、供电节点等，实现了管用分离。

附件2

伊朗油轮事件背后的卫星互联网暗战：iDirect设备测绘与安全风险研究

一、前言

本文主要分享一些我们最近对iDirect设备的研究，篇幅较长，我们公开了部分研究成果，也希望更多对卫星网络安全研究感兴趣的读者能加入这个新赛道。

二、事件回顾

2.1. 事件概况

2025年3月18日，黑客组织Lab Dookhtegan（又称“Read My Lips”）宣称对伊朗两大国有航运公司—伊朗国家油轮公司（NITC）和伊斯兰共和国航运公司（IRISL）的116艘船只发动大规模网络攻击，导致油轮的卫星通信系统全面瘫痪。此次攻击正值美国对也门胡塞武装发动军事打击之际，被外界视为针对伊朗地区代理人的“数字报复”。

此次攻击主要针对船舶的卫星通信系统，导致船上和陆地间的通信中断，该组织利用Shodan等互联网搜索工具扫描并锁定了暴露在互联网上的iDirect卫星通信终端，通过默认口令获取终端root权限。攻击者随后部署自动攻击脚本，利用终端自带的dd指令擦除存储器，导致终端系统无法正常工作。

本次攻击事件的技术复杂度表明，这绝非普通黑客组织所能独立完成，背后可能存在国家行为体的间接支持。Lab Dookhtegan 在Telegram上表示，发起这项行动是为了配合美国对也门胡塞武装的袭击，这两家公司负责向胡塞武装供应弹药。根据技术分析，此次攻击手法与2022年2月针对Viasat卫星网络的攻击高度相似，同样利用了设备弱口令和系统版本陈旧(2020年版本)的安全缺陷，反映了卫星通信设备面临的普遍安全挑战。

2.2.冲突焦点

在此次事件中，美国ST Engineering iDirect公司的iDirect卫星调制解调器成为攻击者的核心目标。作为船舶与外界通信的关键桥梁，iDirect卫星调制解调器在船只远离陆地时提供可靠的高带宽通信链路。这些设备采用"星状网"拓扑结构，通过Ka或Ku波段与地球同步轨道卫星相连，形成覆盖全球海域的通信网络，在伊朗海事领域有大量部署。iDirect卫星调制解调器存在默认口令（root,P@55w0rd!），一般用户不会主动修改该密码导致默认口令的风险存在。另一方面，系统版本的陈旧也增加了较大风险，通过此次事件获取到的信息，该设备系统为2020年版本，OpenSSH等关键服务版本老旧，主要由于设备厂商较少提供系统更新服务导致，这些脆弱性与设备厂商缺乏持续更新支持直接相关，造成"技术债务"不断积累。

从功能角度看，这些卫星终端负责船舶的互联网接入、远程监控、船员通信及数据传输等关键业务。虽然目前多数船只的总线系统与通信系统相对隔离，限制了攻击影响范围，但随着船舶自动化程度提高和系统互联深化，这种隔离正逐渐弱化。攻击者通过破坏这些终端，不仅造成通信中断，还展示了针对关键基础设施的精准打击能力。美国企业生产的卫星通信设备在伊朗油轮上的广泛应用，形成了一种特殊的技术依赖关系，使伊朗关键海运基础设施在国际政治博弈中处于脆弱位置。

三、海事卫星通信骨干单元iDirect设备

3.1. iDirect设备简介

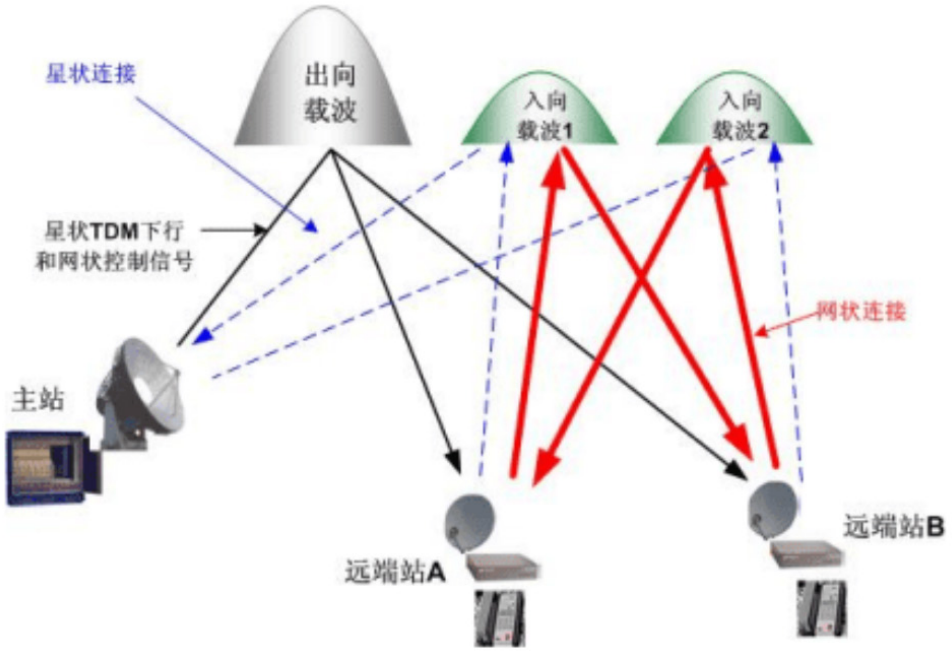
iDirect设备指的是美国ST Engineering iDirect公司（其母公司为新加坡ST Engineering）的卫星通信产品。ST Engineering iDirect产品类型包括调制解调器、集线器和卫星通信解决方案，主要服务于服务商、网络运营商、政府机构、大型企业、军队等客户，其全资子公司iDirect Government是美国国防部领先的卫星通信产品供应商。其产品线涵盖iQ系列、Evolution系列、Evolution Defense 系列、Velocity 系列、MDM系列及9系列等多个方向，其中Evolution系列主要用于星状组网架构的VSAT场景，在海事通信领域具有广泛应用。消息表明，我国目前仍有Evolution系列的设备正在服役。

iDirect相关设备并不依赖于特定的卫星系统，而是通过与不同的卫星服务提供商合作，使用多种卫星来提供通信服务。伊朗的油轮具体使用哪颗卫星来提供通信服务取决于服务提供商的选择和船舶的航行区域。此次攻击的核心目标是船载iDirect VSAT（甚小孔径终端）卫星通信设备中的调制解调器。

iDirect　VSAT设备的工作原理基于卫星通信的基本架构，实现了地面站点与卫星之间的双向数据传输。其通信链路包括从中心站点（Hub）到远程站点的前向链路和从远程站点回传到中心站点的返回链路。

其技术特点是采用基于TDMA（时分多址）和SCPC（单载波每信道）的混合访问方式：支持DVB-S2/S2X标准，实现高效的带宽利用；实现动态带宽分配(DBWA)，根据流量需求自动调整带宽资源；集成QoS(服务质量)功能，确保关键业务流量优先处理。采用IP封装技术，将用户数据封装成适合卫星传输的格式，实现加密和压缩功能，保障数据安全和传输效率，支持TCP加速和Web缓存，优化卫星链路的数据传输性能。

其网络架构由中心主站、卫星转发器和远程终端组成，主站连接互联网骨干网，负责管理整个网络，远程终端通过天线和调制解调器与卫星通信。



3.2. 主要部署场景与应用生态

iDirect在全球范围内实现了可靠的卫星通信，特别是在传统通信基础设施不可用或不可靠的地区发挥着重要作用,如在海事通信、能源行业、政府和军事应用、偏远地区连接等场景下应用。

在海事领域，iDirect设备广泛应用于海上通信。可用于商业船队，为船员提供互联网访问和通信服务，支持船舶远程监控和诊断系统，提供航线优化和天气导航信息服务；也可用于邮轮和客运船，为乘客提供高速互联，支持船上娱乐系统和支付系统，实现船舶安全监控和紧急通信；还可用于海上石油平台，提供远程操作和监控能力，支持视频会议和专家远程协助，确保关键业务数据的实时传输。

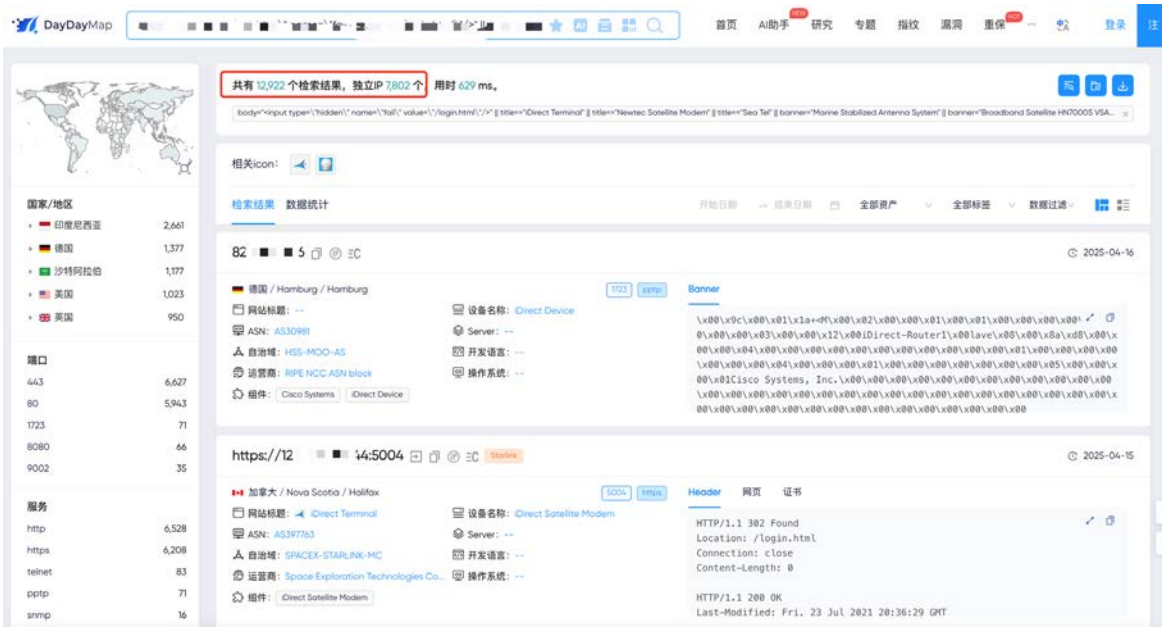
在石油和天然气行业，iDirect设备可应用于偏远油气田的通信和管道监控等场景。可连接偏远油气田现场与总部的通信，支持SCADA系统和远程监控，提供员工福利通信服务；可用于管道监控，实现长距离管道的实时监控，支持泄漏检测系统数据传输，提供安全监控和紧急响应通信。

在政府和军事领域也有广泛应用。iDirect的军用级产品线可应用于战术通信，提供易于部署的机动通信系统，支持加密和抗干扰通信，实现指挥控制系统的网络化；还可应用于边境监控，连接偏远监控站点，支持视频监控和传感器数据回传，提供紧急情况下的通信保障。

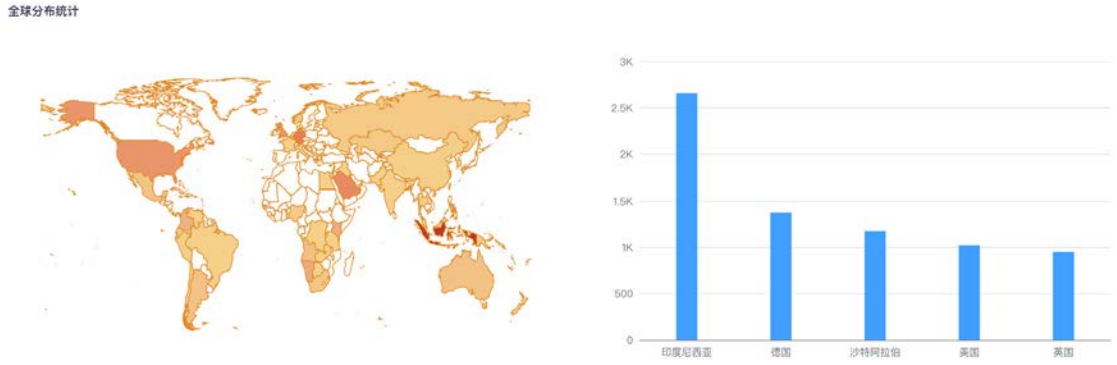
在缺乏传统通信基础设施的偏远地区通信方面也有着应用。可在缺乏传统通信基础设施的地区提供互联网接入，支持远程教育和医疗服务，实现政府公共服务的数字化；在灾难响应场景下，可以提供快速部署的应急通信系统，支持救灾指挥和协调以及在传统通信中断时提供备份连接。

3.3. 互联网设备分布情况

从DayDayMap的测绘结果显示，共有12922个设备暴露在互联网上。



其中印尼、德国、沙特、美国和英国使用的该设备最多，这些国家也都对应有大量的海上通信业务。



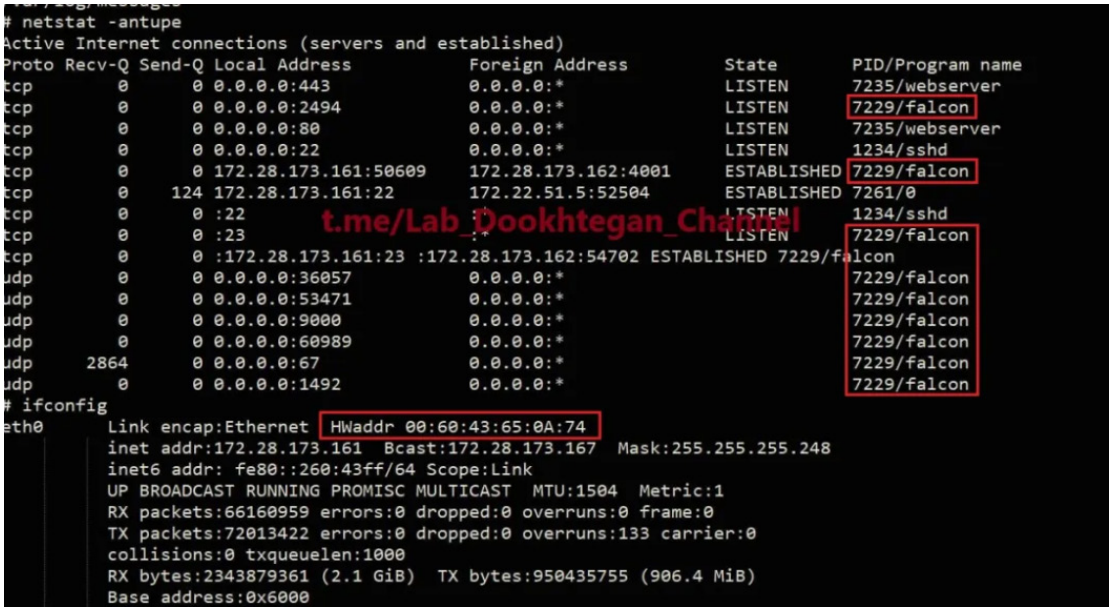
四、iDirect设备相关协议分析

4.1. 分析思路

iDirect设备提供的协议从多个方面进行分析，一个是根据伊朗反政府黑客组织“Lab　Dookhtegan”公布的信息；另一个是设备的官方文档；三是根据设备的应用场景入手；最后通过未知协议带有特定信息入手。

4.1.1. 根据伊朗反政府黑客组织“Lab Dookhtegan”公布信息

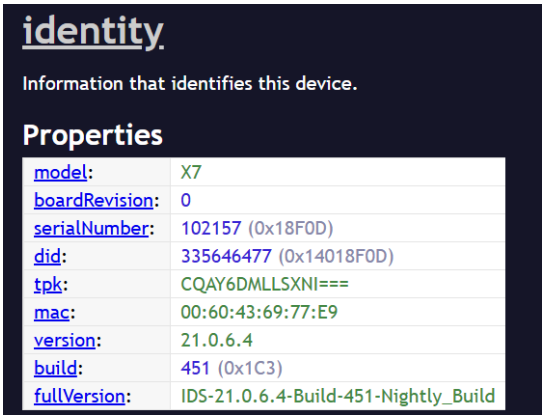
根据伊朗反政府黑客组织“Lab　Dookhtegan”公布的iDirect设备内部监听端口信息可知，目前TCP端口443，80，22，2494，以及UDP端口36057，53471，9000，60989，67，1492均有机会对其进行尝试。

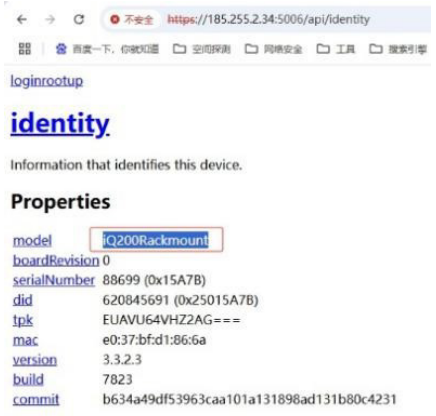


A、80，443webserver

在daydaymap上根据如下指纹搜索到相关设备，其中title=="iDirect Terminal"可以确认是该产品，而另一个无法对其进行确认。

```
body="<input type=\"hidden\" name=\"fail\" value=\"/login.html\"/>"||title=="iDirect Terminal"
```





This chapter describes how to log in to Web iSite and how to load the remote image software package on the X1, X7, and e150 Satellite Routers.

9.1 Logging In to Web iSite

Perform the steps in the following section to establish communication with the Satellite Router using Web iSite.

To log in:

1. Connect a crossover or straight-through Ethernet cable between the LAN port of the local PC and the LAN port of the Satellite Router. (For an Evolution X7, connect to the port labeled LAN 1.)
2. Open a Web browser.
3. Enter the IP address of the Satellite Router into the address bar of the Web browser in the following format:

   `https://IP Address/`

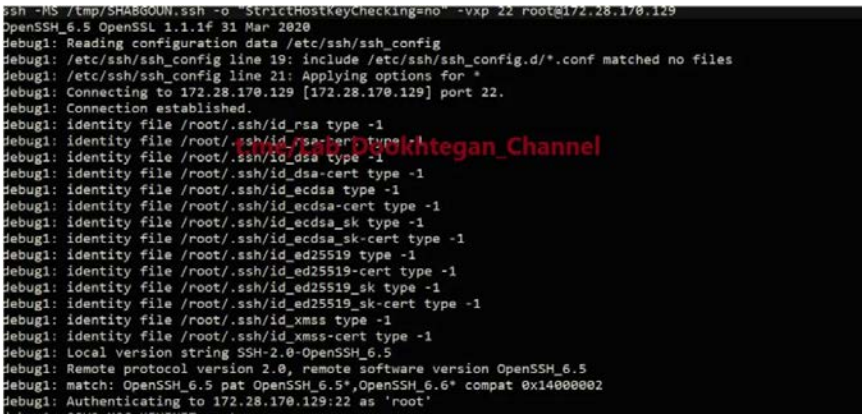
   where *IP Address* is the IP address of the Satellite Router. See Figure 27.

Figure 27. Connecting to the Satellite Router using Web iSite

Figure 28. Web iSite Login Page

Note: The factory default admin password is iDirect. However, after an options file has been loaded and the Satellite Router has been reset, the password changes to match the password in the options file.

B、22端口的ssh信息



C、Falcon主要是用于运行所有的satellite functions。

> *service idirect_falcon restart*

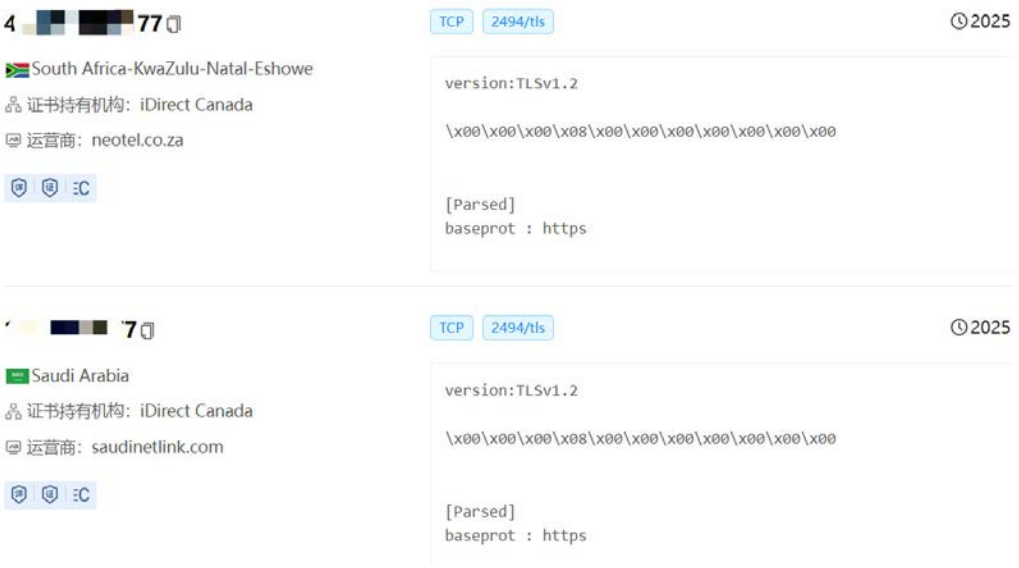
This will temporarily take your remote offline, but it is needed to make the changes. This will wrap up most of the fun you will end up having in linux.

iDirect calls the service that runs all of the satellite functions on your remote, the falcon service. To get into the falcon service, type "telnet 0" from the linux command line. From there you can run a series of commands to find the satellite information you are used to looking for. Here are a couple examples:

```
[RMT:17231] admin@telnet:127.0.0.1;4494
> rx power
Rx Power: -66.830002

[RMT:17231] admin@telnet:127.0.0.1;4494
> rx snr
Rx SNR: 11.930000
```

```
# cat falcon.opt | more
[BTP]
        device_mode = tdma
        device_name = btp
        device_path = /dev

[BTP_REQ]
        device_mode = tdma
        device_name = btp_req
        device_path = /dev

[COMPRESSION]
        Threshold = 90

[DEBUG]
        cpu_util_test_enabled = 0

[DVBS2]
        frame_length = 0.0
        frame_size = short
        inroute_frame_length = 125.000000
        mode = acm
        ncr_interval = 3375000
        pilot = 1
--More--
```

在2494端口探测数据时发现有iDirect证书的数据，用于佐证2494端口对iDirect设备的识别。

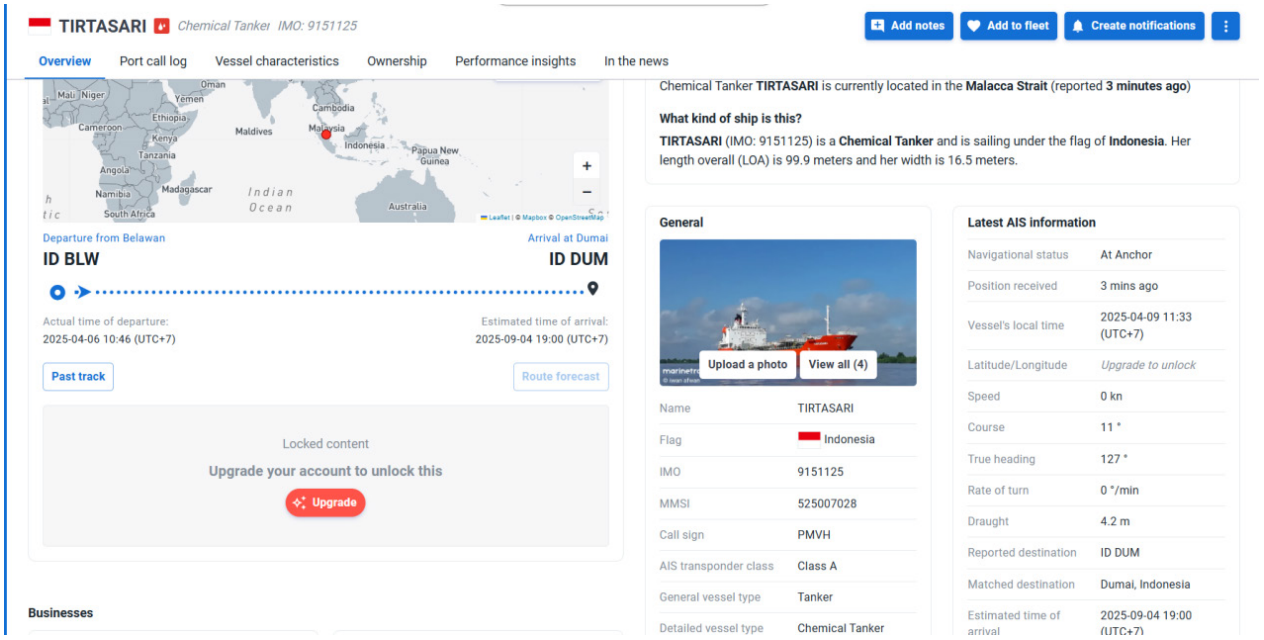


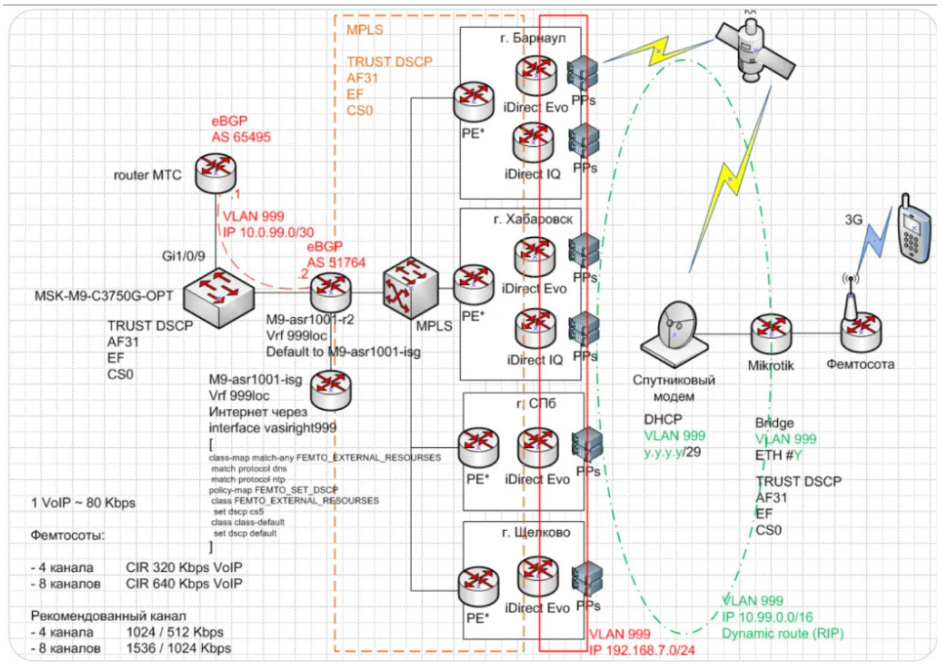
4.1.2. iDirect Velocity的说明书发现其支持snmp功能

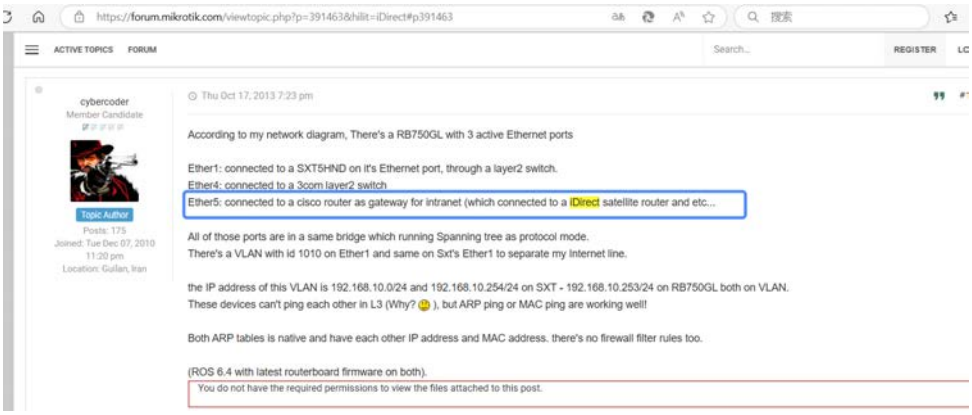
4.2. 设备的应用场景

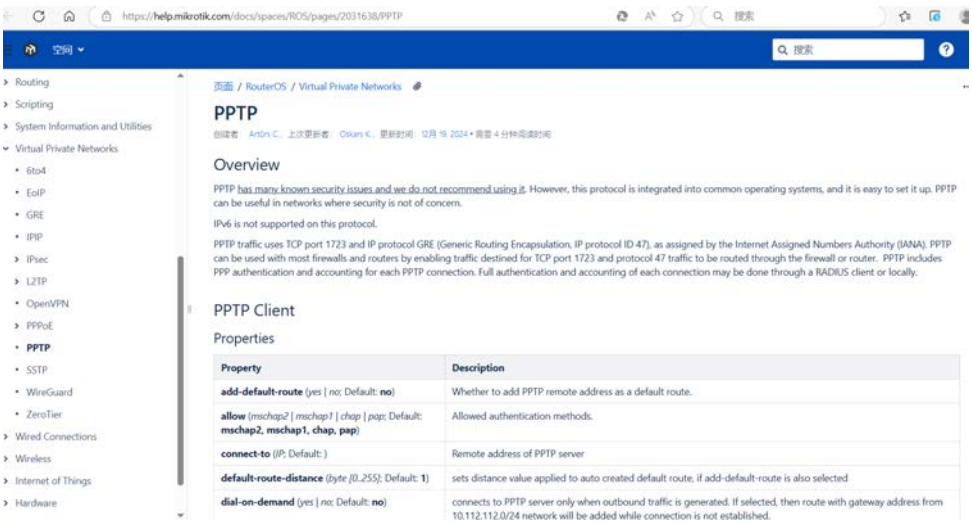
i. Mikrotik

从《俄罗斯Dozor-Teleport卫星通信运营商遭黑中断情况分析》一文中发现了iDirect与Mikrotik混合的应用场景，同时在其Mikrotik官网论坛里发现用户关于iDirect和Mikrotik混合场景的讨论。再根据Mikrotik提供的协议，进行涉及协议的分析。如下图，可以获取到这个设备的hostname,当将TIRTASARI在海事网站MarineTraffic: Global Ship Tracking Intelligence | AIS Marine Traffic进行搜索时，可以发现这是一艘货轮的名称。




MPLS
TRUST DSCP
AF31
EF
CS0
eBGP
AS 65495
router MTC
.1
VLAN 999
IP 10.0.99.0/30
Gi1/0/9
.2
eBGP
AS 31764
MSK-M9-C3750G-OPT
TRUST DSCP
AF31
EF
CS0
M9-asr1001-r2
Vrf 999loc
Default to M9-asr1001-isg
MPLS
M9-asr1001-isg
Vrf 999loc
Интернет через
interface vasiright999
[
class-map match-any FEMTO_EXTERNAL_RESOURCES
match protocol dns
match protocol ntp
policy-map FEMTO_SET_DSCP
class FEMTO_EXTERNAL_RESOURCES
set dscp cs5
class class-default
set dscp default
]
1 VoIP ~ 80 Kbps
Фемтосоты:
- 4 канала CIR 320 Kbps VoIP
- 8 каналов CIR 640 Kbps VoIP
Рекомендованный канал
- 4 канала 1024 / 512 Kbps
- 8 каналов 1536 / 1024 Kbps
г. Барнаул
iDirect Evo
PPs
PE*
iDirect IQ
г. Хабаровск
г. СПб
г. Щелково
VLAN 999
IP 192.168.7.0/24
Спутниковый
модем
DHCP
VLAN 999
y.y.y.y/29
Mikrotik
Фемтосота
3G
Bridge
VLAN 999
ETH #Y
TRUST DSCP
AF31
EF
CS0
VLAN 999
IP 10.99.0.0/16
Dynamic route (RIP)

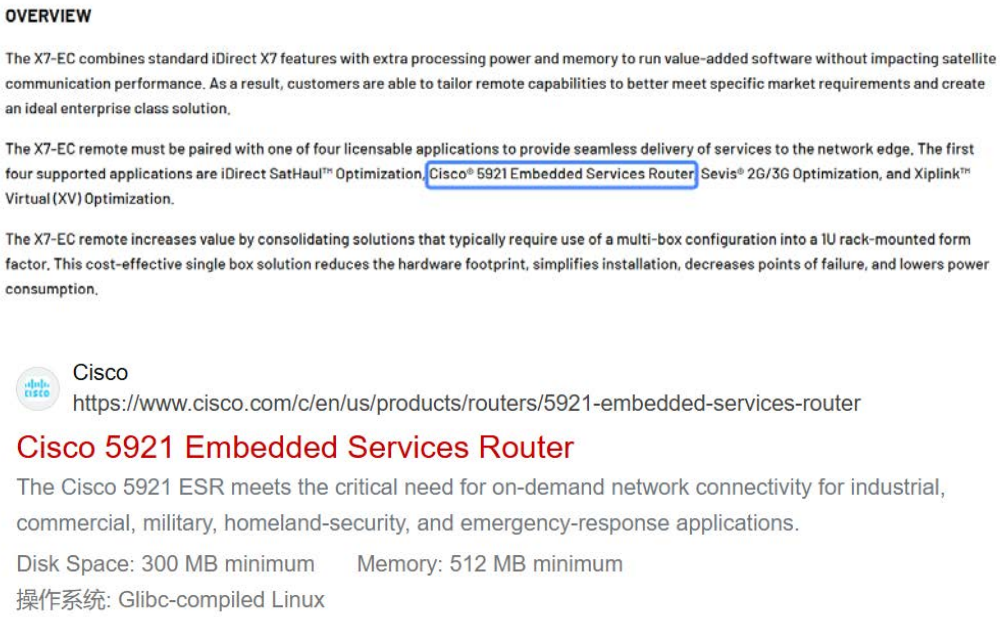

https://forum.mikrotik.com/viewtopic.php?p=391463&hilit=iDirect#p391463
ACTIVE TOPICS
FORUM
REGISTER
cybercoder
Member Candidate
Topic Author
Posts: 175
Joined: Tue Dec 07, 2010 11:20 pm
Location: Guilan, Iran
Thu Oct 17, 2013 7:23 pm
According to my network diagram, There's a RB750GL with 3 active Ethernet ports
Ether1: connected to a SXT5HND on it's Ethernet port, through a layer2 switch.
Ether4: connected to a 3com layer2 switch
Ether5: connected to a cisco router as gateway for intranet (which connected to a iDirect satellite router and etc...
All of those ports are in a same bridge which running Spanning tree as protocol mode.
There's a VLAN with id 1010 on Ether1 and same on Sxt's Ether1 to separate my Internet line.
the IP address of this VLAN is 192.168.10.0/24 and 192.168.10.254/24 on SXT - 192.168.10.253/24 on RB750GL both on VLAN.
These devices can't ping each other in L3 (Why?), but ARP ping or MAC ping are working well!
Both ARP tables is native and have each other IP address and MAC address. there's no firewall filter rules too.
(ROS 6.4 with latest routerboard firmware on both).
You do not have the required permissions to view the files attached to this post.

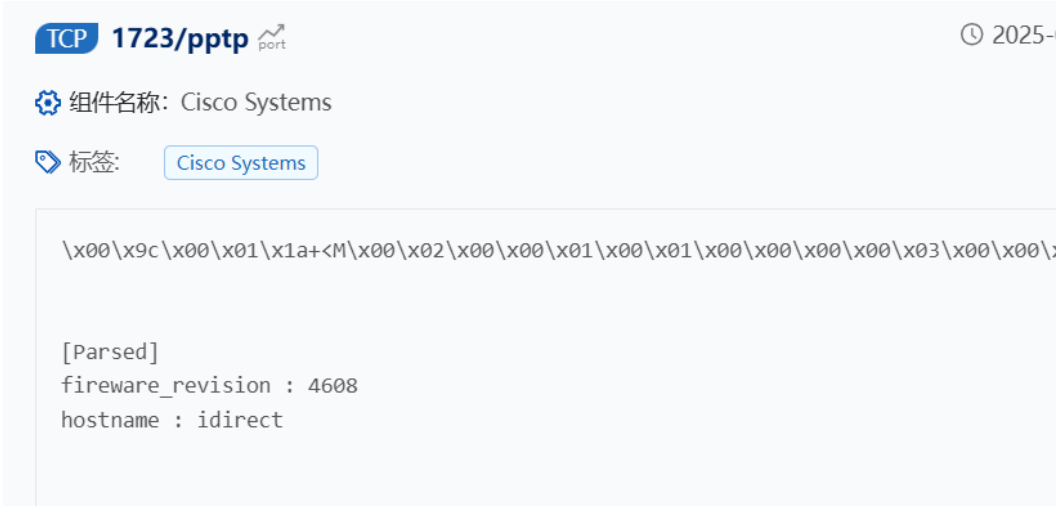

https://help.mikrotik.com/docs/spaces/ROS/pages/2031638/PPTP
Routing
Scripting
System Information and Utilities
Virtual Private Networks
6to4
EoIP
GRE
IPIP
IPsec
L2TP
OpenVPN
PPPoE
PPTP
SSTP
WireGuard
ZeroTier
Wired Connections
Wireless
Internet of Things
Hardware
页面 / RouterOS / Virtual Private Networks
PPTP
Overview
PPTP has many known security issues and we do not recommend using it. However, this protocol is integrated into common operating systems, and it is easy to set it up. PPTP can be useful in networks where security is not of concern.
IPv6 is not supported on this protocol.
PPTP traffic uses TCP port 1723 and IP protocol GRE (Generic Routing Encapsulation, IP protocol ID 47), as assigned by the Internet Assigned Numbers Authority (IANA). PPTP can be used with most firewalls and routers by enabling traffic destined for TCP port 1723 and protocol 47 traffic to be routed through the firewall or router. PPTP includes PPP authentication and accounting for each PPTP connection. Full authentication and accounting of each connection may be done through a RADIUS client or locally.
PPTP Client
Properties
Property
Description
add-default-route (yes | no; Default: no)
Whether to add PPTP remote address as a default route.
allow (mschap2 | mschap1 | chap | pap; Default: mschap2, mschap1, chap, pap)
Allowed authentication methods.
connect-to (IP; Default:)
Remote address of PPTP server
default-route-distance (byte [0..255]; Default: 1)
sets distance value applied to auto created default route, if add-default-route is also selected
dial-on-demand (yes | no; Default: no)
connects to PPTP server only when outbound traffic is generated. If selected, then route with gateway address from 10.112.112.0/24 network will be added while connection is not established.

Mikrotik一般在外部的协议主要是PPTP,L2TP,IPsec以及bandwidth-test。其中pptp和l2tp协议能获取更多有效信息供指纹进行识别。

ii. Cisco

iDirect X7-EC Satellite Router内嵌了Cisco 5921 Embeded services Router，也就是说可以通过Cisco端口进行iDirect设备的识别。



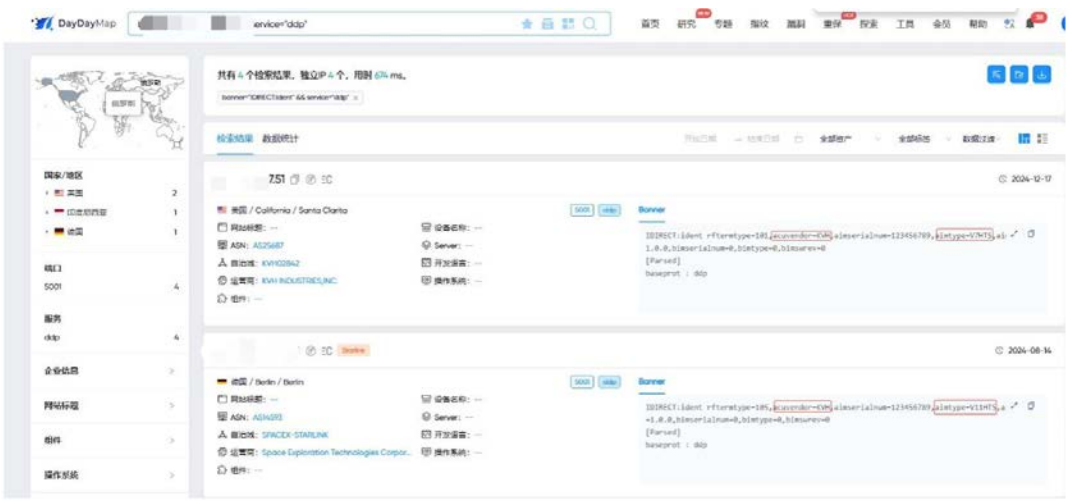


未知协议

```
banner="iDIRECT"&&service="junoscript"
```

banner="IDIRECT:ident" && service="unknown"

对内容进行分析后发现，KVH V7-HTS是真实的VSAT设备



KVH
https://www.kvh.com/products/connectivity/vsat-systems/tracphone-v7hts

TracPhone V7-HTS - KVH Compact, powerful VSAT antenna

5 天之前 · The 3-axis, gyro-stabilized, 60 cm (24 inch) diameter TracPhone® V7-HTS offers blazing fast, worldwide connectivity via next-generation satellites on KVH's global HTS …

Investors

KVH Industries, Inc. (Nasdaq: KVHI) creates and delivers the innovations that enable our mobile world. A global leader in mobile connectivity, our g…

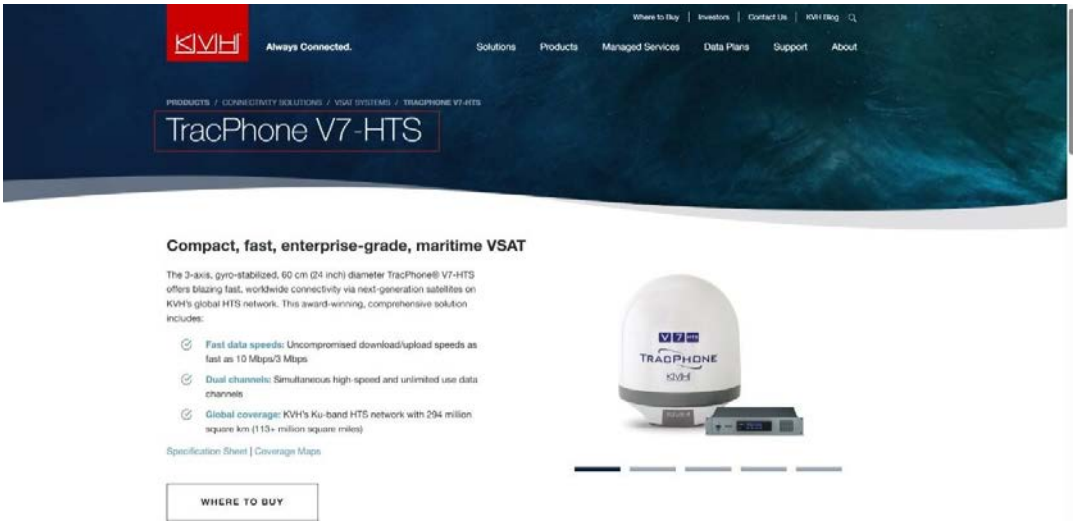
仅显示来自 kvh.com 的搜索结果

丽赫国际
https://www.bihec.com/kvh/船载vsat通信系统-kvh...

船载VSAT通信系统 KVH TracPhone V7-HTS 指南针传感器 ...

2020年2月28日 · 用户友好的管控：通过myKVH™ mini-VSAT Manager这个综合性的工具，完全透明地控制数据使用、管理操作和个人使用。 ·容易设置给船上每个人的、每日或每月的上网 …

预计阅读时间：3 分钟

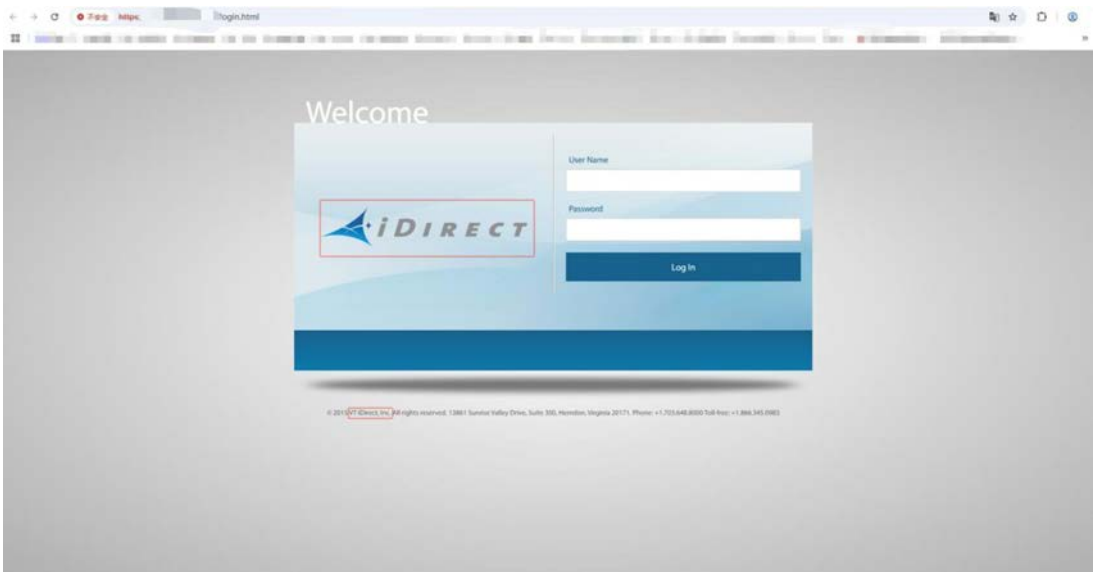


五、iDirect设备指纹特征

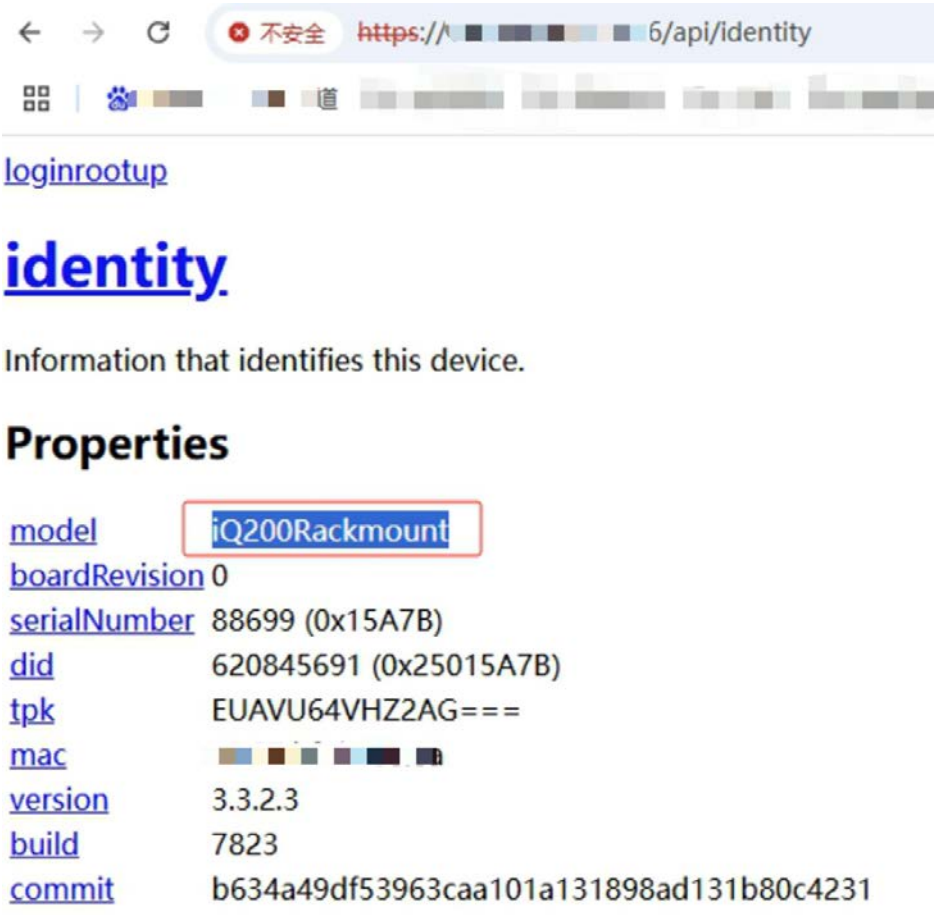
iDirect设备相关指纹特征包括：http/https协议指纹、PPTP协议指纹、title类指纹、banner类指纹、组织类指纹。在DayDayMap平台搜索单一指纹特征或组合指纹特征，可进行iDirect设备确认。考虑到信息敏感性，以下章节部分检索指纹已做模糊处理。

5.1. http/https协议指纹特征

A、在daydaymap平台搜索title=="iDirect Terminal"

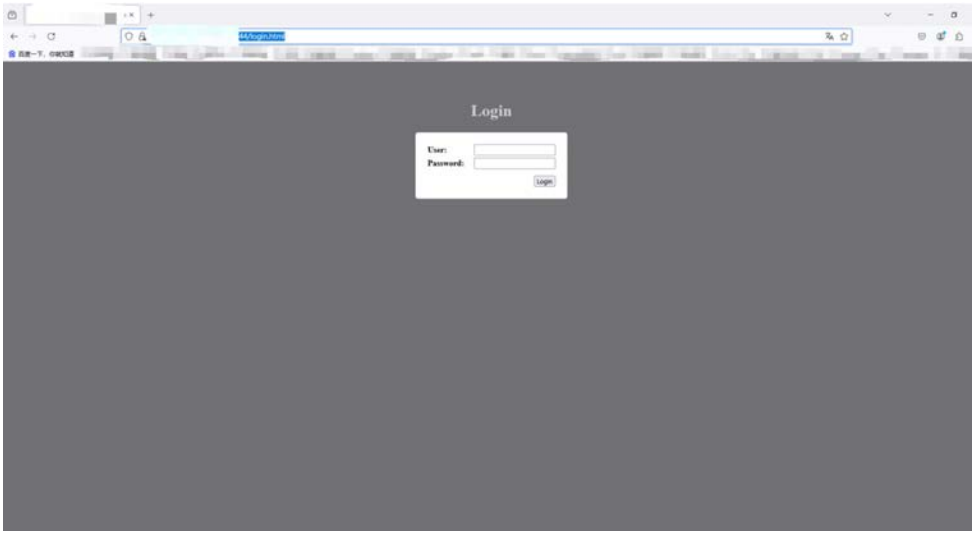


可以看到是iDirect公司的设备，继续研究发现可以进一步获取到设备型号：

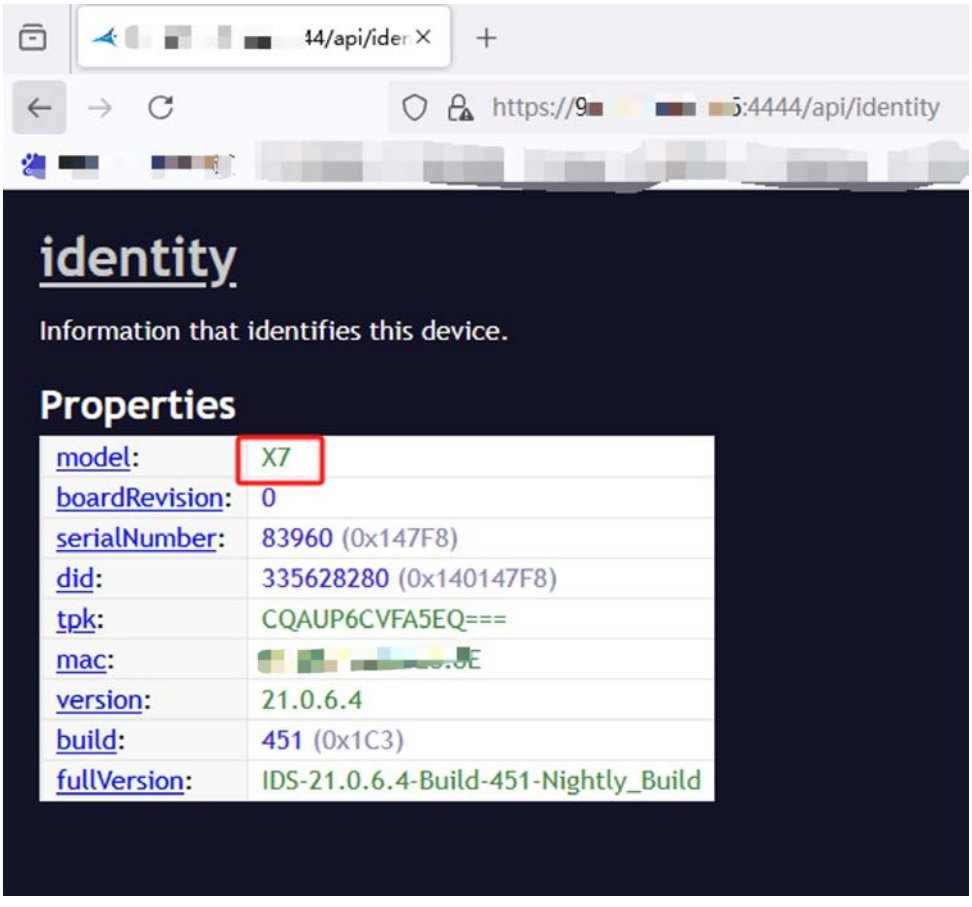


该型号是iDirect的一款卫星调制解调器：

B、在daydaymap平台搜索body="*****码住)login.html\"/>"，结合iDirect　Evolution路由器说明书可以看到web登录页面如下：

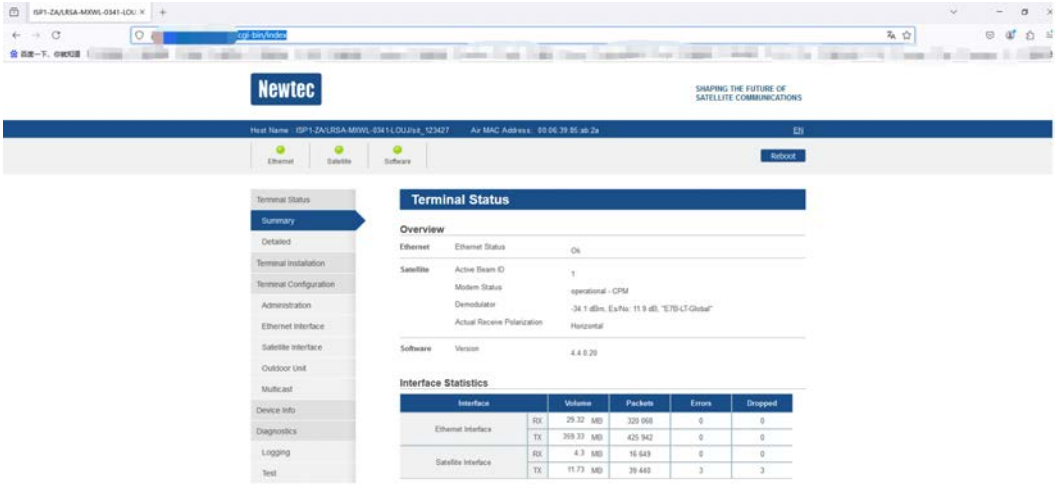


继续研究可以获取到设备型号：

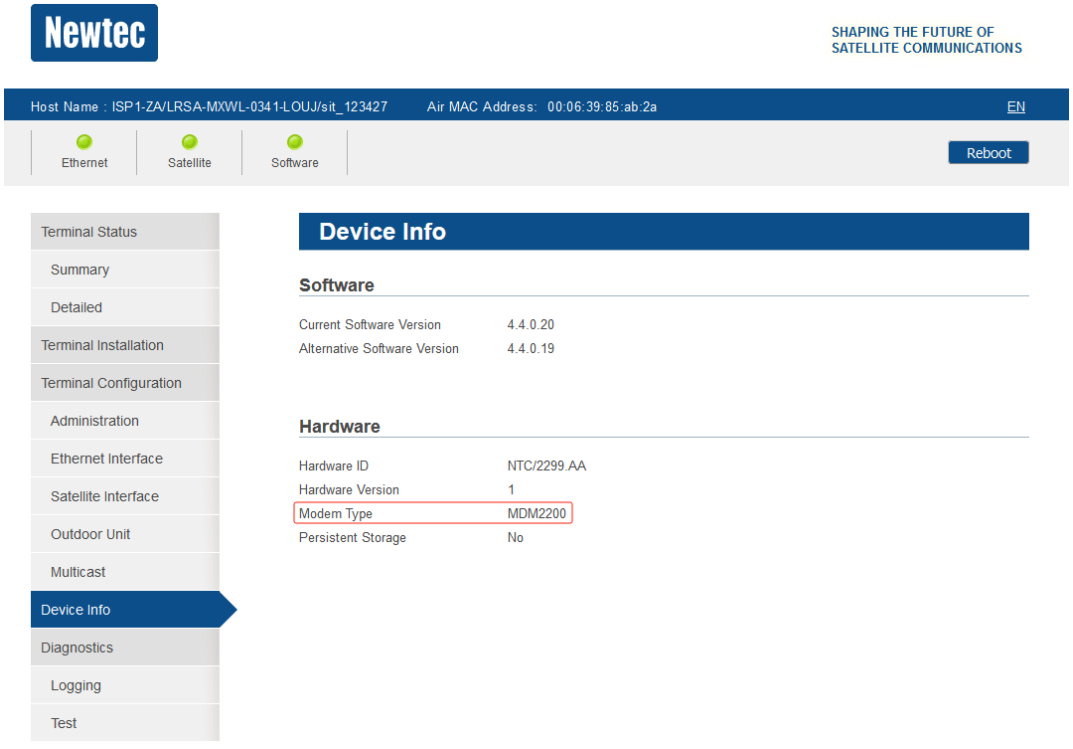


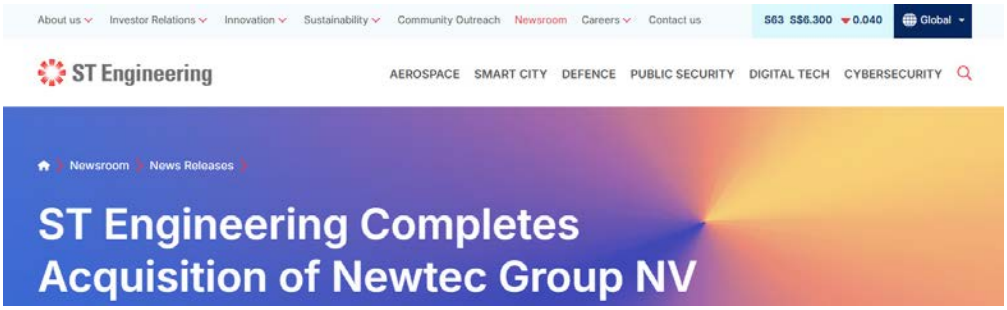
可以看到是iDirect Evolution X7卫星路由器设备。

C、在daydaymap平台搜索title=="Newtec Satellite Modem"

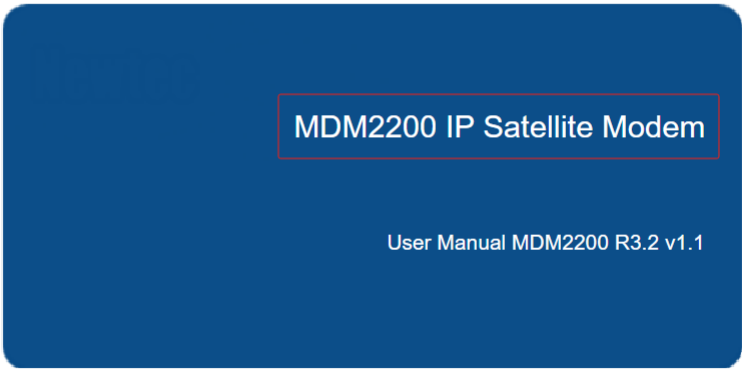


点击页面的Device Info，可以看到设备型号：





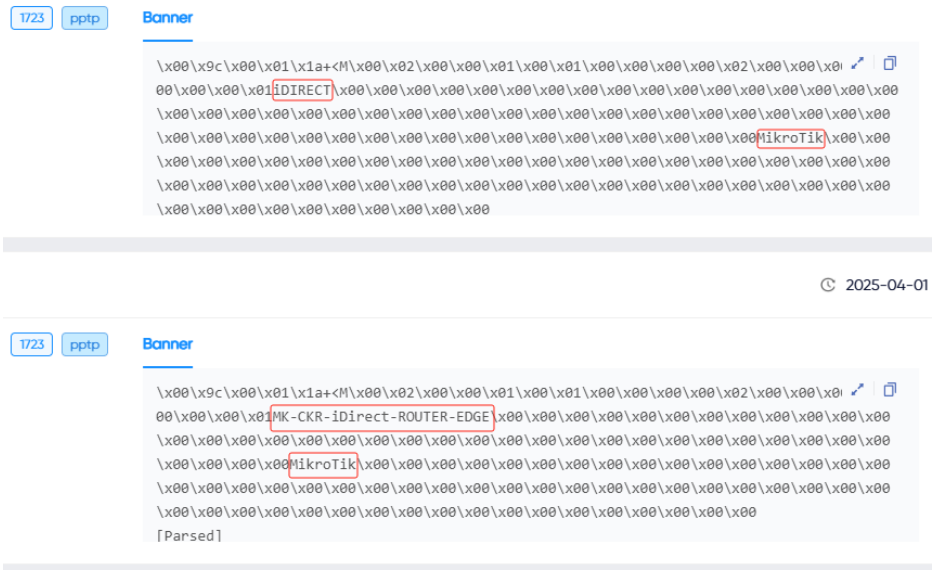
Download this manual



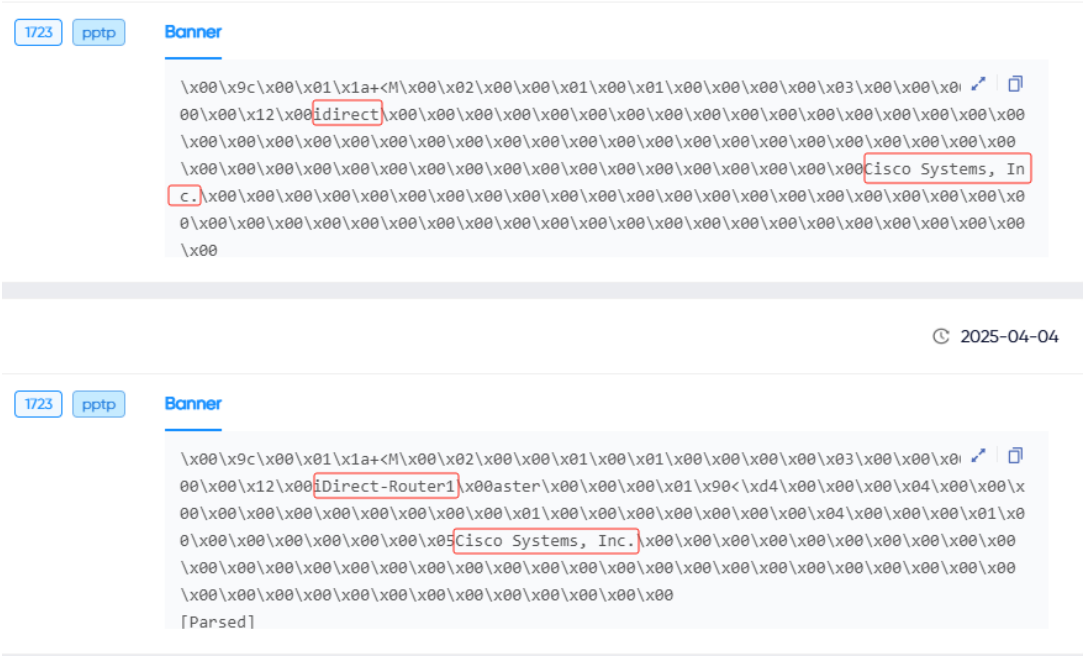
可以看到ST Engineering把Newtec收购了，Newtec MDM2200是卫星调制解调器设备。

5.2. pptp协议指纹特征

在daydaymap平台搜索banner="iDirect" && service="pptp"，主要有两个厂商的路由器会出现在iDirect设备系统中，MikroTik和Cisco。MikroTik的指纹特征如下：

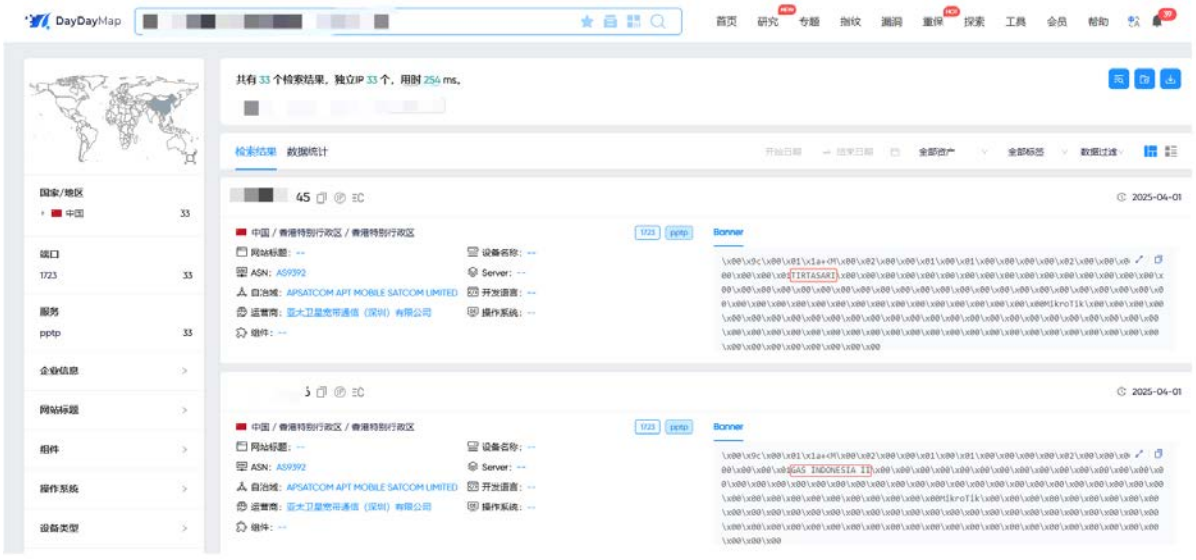


Cisco的指纹特征如下：



1、org组织指纹特征

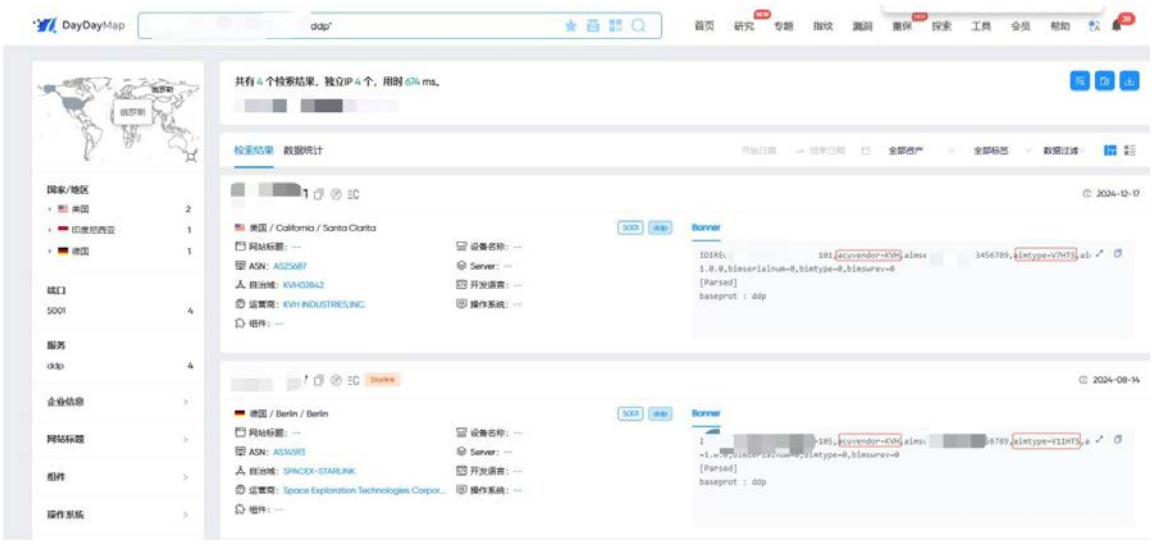
在daydaymap平台搜索org:"APT MOBILE *****(码住)" && service="pptp"，数据中的主机名是船的名字：



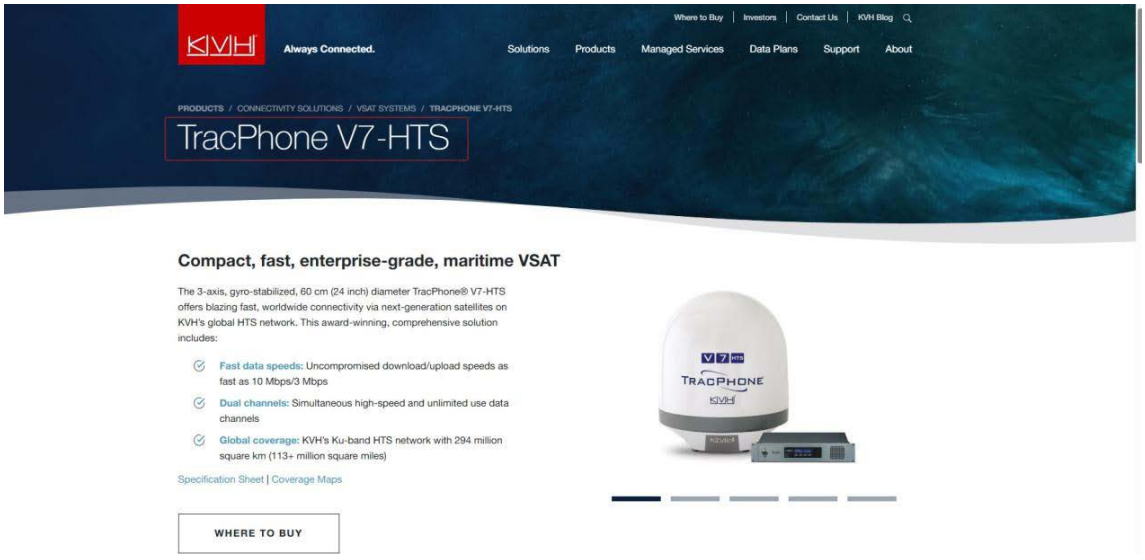
这些船名字在https://www.marinetraffic.com/en/ais/home/centerx:25.2/centery:-51.6/zoom:4网站上搜索船的名字，可以看到船的位置信息。

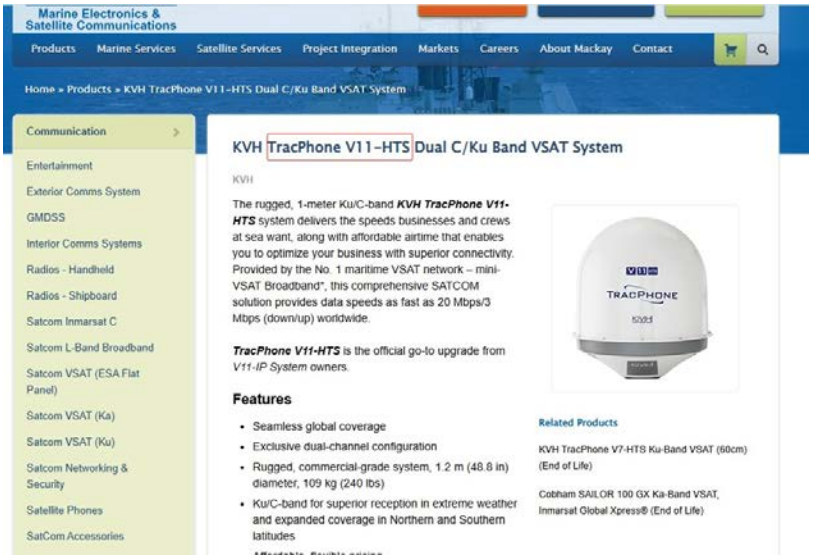
2、其他iDirect相关设备指纹特征

A、在daydaymap平台搜索banner="IDIRECT: *****(码住)" && service="ddp"

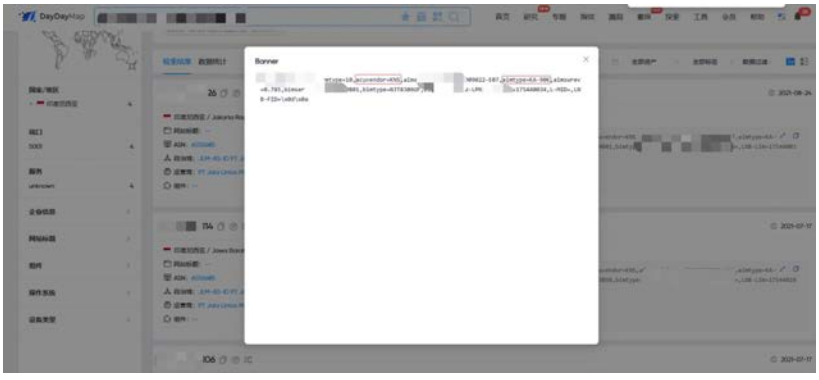


可以看到厂商以及设备型号，结合搜索引擎得知是VSAT系统设备：





B、在daydaymap平台搜索banner="IDIRECT: *****(码住)" && service="unknown"，能够发现一些未知协议信息



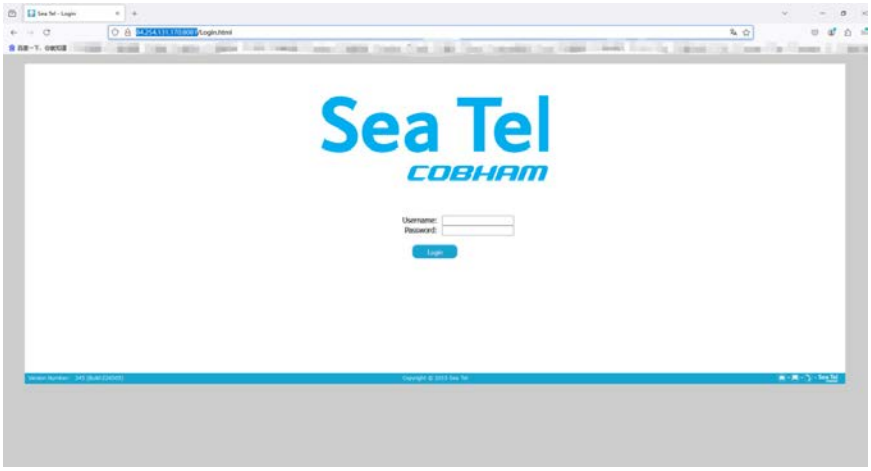
taiwanagriweek.com
https://www.taiwanagriweek.com/catalog-detail/10947
KNS 船載天線 Z10MK4 Ka/Ku-Band Maritime …
採用先進的 Ka/Ku 波段頻率，此天線系統提供卓越的頻寬連接，確保在各種海洋環境中（包括商業船隻、豪華遊艇和離岸平台）穩定可靠的通訊。 其堅固設計、先進的追蹤技術和易於安裝，使其成為現代海上通訊需求的理想選擇。 先進的 …

electromarinaservice.com
https://electromarinaservice.com/product/x-vsat
X-vsat Communications | Electromarina Service …
KNS has the capability of providing exceptional military standard service for secure broadband connectivity, voice, data, video and TV Services, at very competitive prices. Με κεραίες KNS VSAT σε MK2 & MK3 KU-KA τώρα έχετε …

KNS Ins.
https://kns-kr.com/english/search/search_board
total search | KNS Inc.
KNS Inc. Partners > Firmware [Mk4 Series] PCU firmware Ver. 2.300 - Enhanced automatic mode in the PCU compass function(add the switching case) input the same heading value about 5 …

NauticExpo
https://www.nauticexpo.cn/prod/kns-35736.html
KNS 品牌展台_海事设备 - _NauticExpo
查看KNS 的所有产品信息和销售点。直接与制造商联系询价，免费获得报价。

C、在daydaymap平台搜索title=="Sea Tel",访问web登录页面如下：



可以看到是Sea Tel的产品，结合Sea Tel官网可以看到Sea Tel的产品也是应用在VSAT系统中：

VSAT系统设备/ Sea Tel 6012

Sea Tel 6012 is a 3-Axis marine stabilized antenna system compatible with most Ku-band satellites. The revolutionary architecture of this 1.5 meter system is based on Sea Tel's industry leading XX09 marine stabilized antenna system. The 6012 is the industry's first 1.5m Ku-band system powered by integrated marine antenna (IMA) software, supplied in a frequency tuned 76" (1.93m) radome or optionally in a 81" (2.05m) radome with air conditioner.

Sea Tel 2400 – High-performance 2.4M Multiband VSAT Innovation shaping the future of connectivity at sea

Unmatched Performance

Maximum uplink power for greater capacity

Sea Tel 2400 is the most powerful 2.4 M VSAT Tri-band antenna. With superior RF architecture and Fibre Optic Technology, you can reach the greatest bandwidth capacity across all frequencies.

Market-leading RF performance »

Market's highest rated payload »

Maximized Scalability

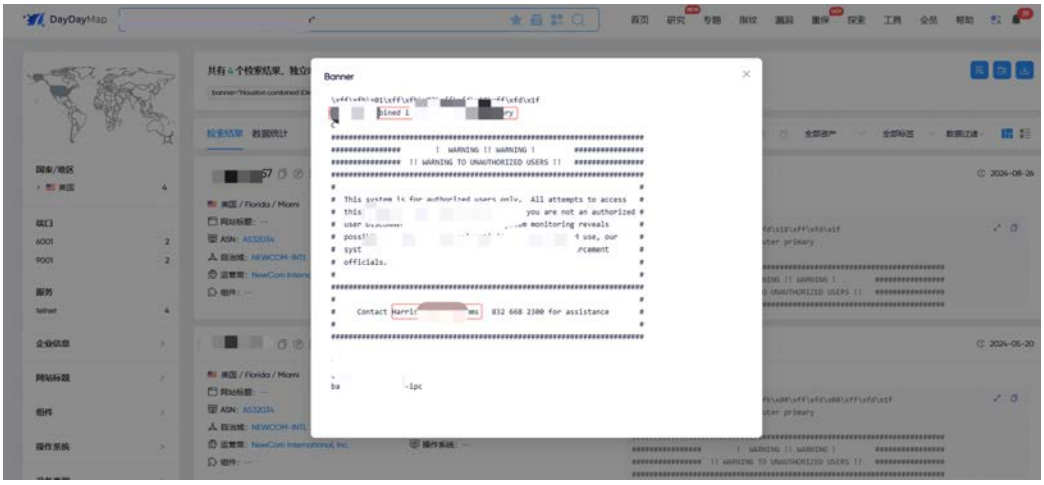
Capabilities on demand for best TCO

Sea Tel 2400 is the market's most flexible 2.4M VSAT antenna platform. With Cobham Satcom's Ka-Band Upgrade Kit and unique Multi-Band Arbitrator, you can customize, scale, and manage your antenna platform on demand across frequencies, networks, and orbits, all while optimizing your antenna's TCO.

Built on dependable, First-to-market 2.4m VSAT Tracking Technology »

Ready for Future Constellations »

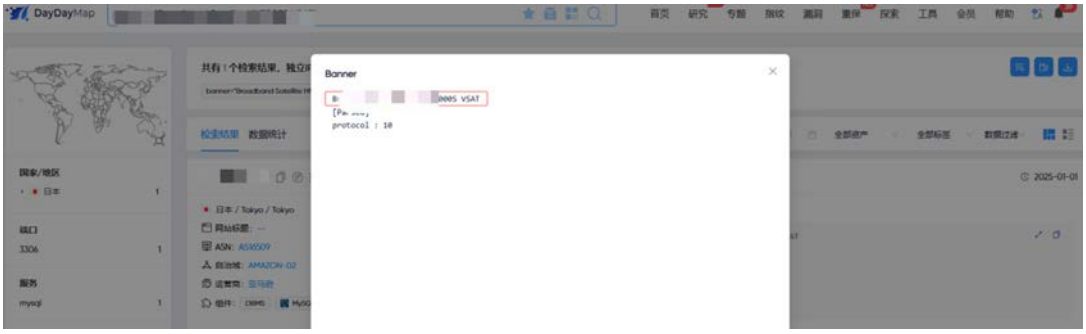
D、在daydaymap平台搜索banner="Houston combined*****(码住)"



可以看到这也是iDirect路由器设备，结合搜索引擎可以得知该厂商也是做卫星互联网相关的设备及解决方案：

Harris CapRock Communications是全球首屈一指的托管卫星与地面通信解决方案提供商，尤其是针对诸如能源、政府和海事市场等偏远与恶劣环境。Harris CapRock拥有并运营着一个强健的全球基础设施，其中包括遍布六大洲的电信港、五座24/7客户支持中心、遍及23个国家/地区的当地办事处，以及遍布北美、中南美、欧洲、西非和亚太地区的超过275个全球现场服务人员支持客户办公点。

E、在daydaymap平台搜索banner="Broadband Satellit*****(码住)"



HN7000S - Scalable, high-performance broadband satellite modem for enterprises

可以看到HN7000S是HUGHES的卫星调制解调器。

六、iDirect设备漏洞信息

6.1. iDirect设备默认口令

6.1.1. ssh默认口令

公开资料表明，此次伊朗油轮事件中，攻击组织Lab Dookhtegan通过iDirect设备弱口令获得root权限，从而导致116艘油轮上的卫星通信中断。iDirect系列调制解调器通常存在默认口令（root,P@55w0rd!），一般用户不会主动修改，从而导致默认口令风险。

6.1.2. Web管理后台默认口令

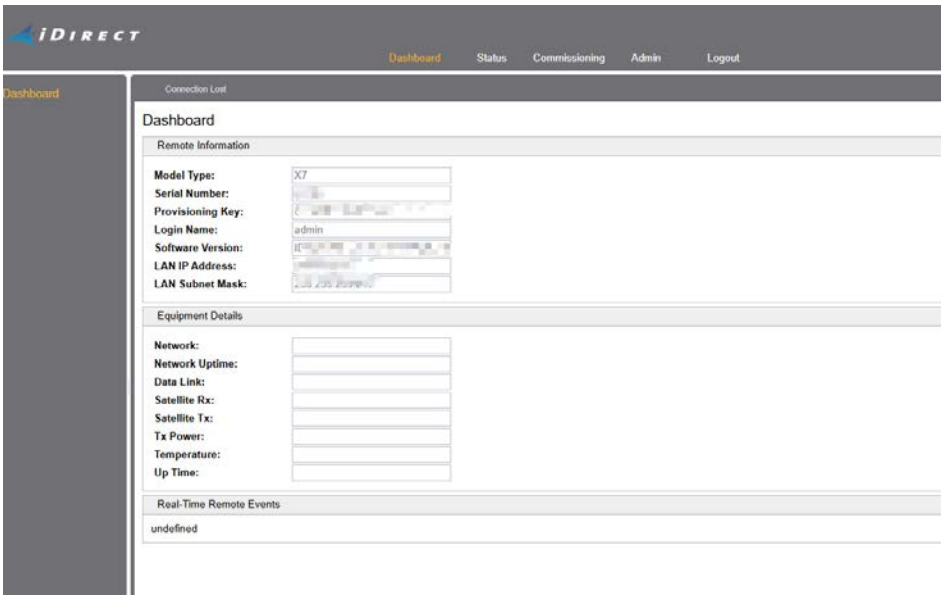
经分析研究，Web iSite是iDirect Evolution系列卫星路由器（如X1、X7和e150型号）内置的Web服务器界面，允许用户通过Web浏览器直接访问和管理这些设备。iDirect Evolution X1路由器基本属性为：

默认登录地址：192.168.0.1

默认登录用户名：Admin

初始密码为：*****(码住)

互联网上暴露的很多web页面并未修改初始密码导致能进入管理后台。相关POC已录制到daydaypoc平台。

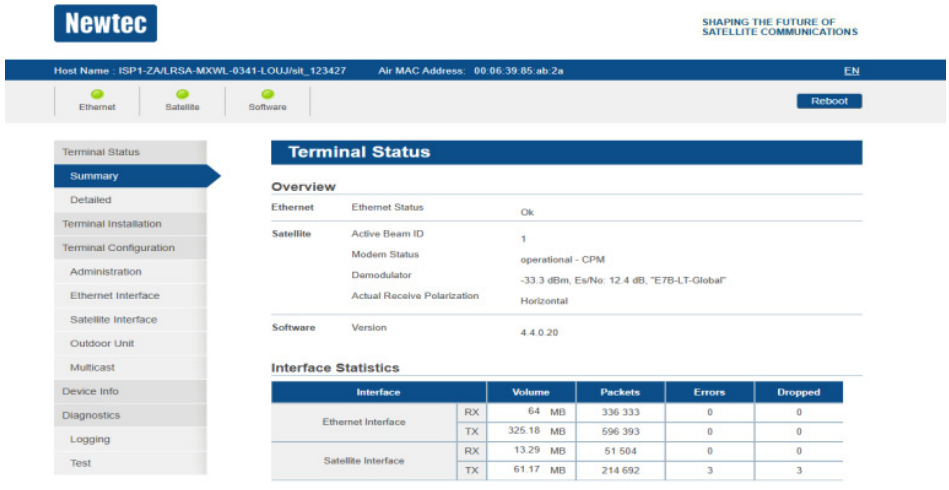


6.2. iDirect设备其他漏洞

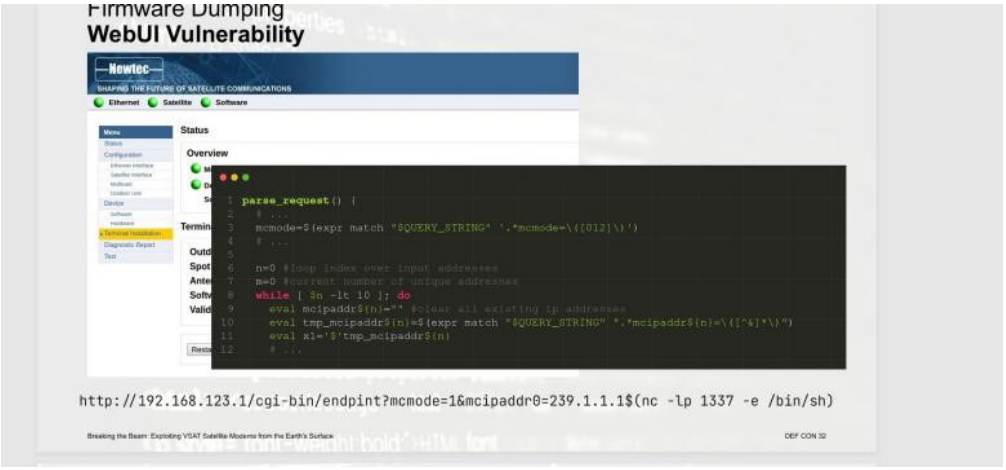
iDirect设备属于ST Engineering公司，该公司收购了Newtec，从前面的测绘分析可以看出，Newtec Satellite Modem与iDirect设备MDM系列相关联。

1、CVE-2024-13502

该漏洞属于Web界面命令注入漏洞，影响的设备为Newtec Satellite Modem，影响的版本是1.0.1.1到2.2.6.19。在管理界面中用于配置多播的‘commit_multicast’页面会将请求中的传入数据传递给bash 脚本中的‘eval’语句导致任意命令执行。经daydaymap测绘验证，可以未授权进入该设备后台：



相关POC已录制到daydaypoc平台，具体如下：



2、CVE-2024-13503

Newtec 更新信号中的基于堆栈的缓冲区溢出导致 RCE，该漏洞显示parse_INFO 函数使用不受限制的“sscanf”将传入网络数据包的字符串读入静态大小的缓冲区中，swdownload 二进制文件中的堆栈缓冲区溢出允许攻击者执行任意代码。

七、油轮到地缘博弈的卫星互联网暗战逻辑

伊朗油轮通信中断事件中，卫星互联网攻击对航运安全的影响受到普遍关注，实质上，此类事件只是冰山一角。随着低轨卫星星座快速铺设，卫星互联网深度嵌入全球通信、导航与信息分发体系，掌握对抗技术主动权的国家，可借助卫星互联网拓展更广泛的地缘触角。

卫星互联网暗战是指国家或非国家行为体通过利用、干扰、劫持、或入侵卫星网络系统，对偏远地区、关键航道、战区前沿、舆论空间等实现低成本、高速度的隐蔽性信息技术干预，借此获得政治、军事、经济优势地位。其对地缘博弈的强化作用，主要体现在以下三方面：

首先，卫星互联网暗战可突破地理边界，实现“全域触达”。卫星互联网不依赖传统地面通信基础设施，无需穿越他国边境或依赖海底光缆，天然具备跨越地理阻隔与主权壁垒的能力，无论是偏远山区、广袤沙漠，还是深海远洋、极地孤岛，卫星互联网都能直接打通“地缘盲区”，让通信“触角”延伸到传统地缘力量难以触达的地方；

其次，卫星互联网暗战可塑造全球认知触角，影响跨境舆论空间。卫星互联网通过全球终端接入，可绕开本地网络安全监管，直接影响不同国家或地区用户的信息来源和上网路径，成为“舆论入口”的新平台，这种“技术通道+认知影响”双维度触角，赋予主导国以跨境信息渗透与舆论操控的潜在能力，正日益成为信息战场的新焦点；

最后，卫星互联网暗战有助于战略前沿外推，地缘防线前置。卫星互联网以其全球可达、实时覆盖的特性，依托低轨星座构建的全球通信体系，使具备主导地位的国家能够远距离感知关键区域动态，部署远程通信压制、数据干扰、电子诱导等“非接触式”对抗手段，从而将战略控制能力由本土边境推向遥远海域、岛链前沿、冲突边缘区。

卫星互联网暗战在地缘博弈中具有不可忽视的作用。它不仅改变了信息传输的传统模式，还赋予国家在全球范围内展开隐蔽战斗、操控舆论、推进战略布局的新能力，成为新时代地缘博弈的重要武器。

八、如何加强卫星互联网防御？

卫星互联网的安全防御是一个复杂的系统工程，涉及到通信链路、卫星设备、网络架构以及地面终端等多个层面。鉴于卫星互联网安全在政治、军事、经济等领域的广泛影响，应高度重视卫星互联网安全防御问题，具体措施包括：

（1）建立网络测绘驱动的卫星互联网安全防御机制

通过部署卫星互联网专用测绘系统，对卫星互联网拓扑结构、节点特征、漏洞风险等进行实时监控，发现卫星互联网设备暴露情况、攻击入口，识别不合规的卫星互联网终端，绘制卫星互联网可视化地图，为卫星互联网安全威胁预警和应急响应处置提供决策依据。

（2）采用成体系的国产化卫星网络通信加密解决方案

在不同类型的卫星通信链路与终端设备中，部署支持国密算法的软硬件加密模块，包括高速、中低速、嵌入式卫星通信密码模块及无人机加密模块，实现多场景、多速率、多平台的通信加密覆盖，提升卫星互联网的体系化安全能力。

（3）研制轻量级的星载边缘AI安全防护模块

针对卫星资源受限的特点，开发低功耗、高实时性的星载边缘AI安全防护模块，通过轻量化神经网络模型与星上数据处理能力，实现卫星互联网的本地化实时安全监测与响应，减少地面站依赖，构建星端协同的智能化安全防护体系。

远江盛邦安全科技集团股份有限公司

热线：4006 911 199

网址：www.webray.com.cn