

NAT技术在调度控制系统改造中的应用研究

提出了一种以NAT技术为核心,综合运用交换机端口镜像、旁听104规约、监听前置服务以及PAT等多种技术实现调度控制系统改造过程中厂站远动信息接入调试的方案,可在不改变厂站端远动机配置且不对旧系统实时数据造成影响的情况下,完成新系统厂站远动信息接入调试,该方案已成功应用于泉州地区电网调度控制系统改造,实际应用情况表明该方案在缩短厂站远动信息接入调试周期,提高新一代调控系统建设效率方面收效显著。

施蔚锦/国网福建电力公司泉州供电公司

0 引言

调度控制系统改造涉及到厂站远动信息的接入调试,由于新旧两套系统的前置数据通信服务器使用不同的调度数据网IP地址,因此需要为每个厂站的远动机增加104规约链路配置,通常需要很大的工作量。以一个220 kV变电站为例,104规约链路配置需要考虑与省调、地调的连接,主调、备调的连接,调控系统双前置服务器的连接,每台前置服务器骨干网双平面地址的连接等四个方面的因素,这样一来每台厂站远动机需要配置的104规约链路数量为16(24)个,造成厂站远动机硬件资源较大的开

销,同时16个链路配置也已经达到了大部分型号的远动机设计的上限,无法再新增链路。由于调控系统改造过程中,新旧两套系统需要并列运行,即厂站远动机需要新增到新系统的104规约链路,显然这给改造工作带来难题。本文提出了一种基于网络地址转换(Network Address Translation, NAT)技术的厂站远动机接入调控系统方案,通过将新旧两套调控系统前置服务器的私网地址进行NAT转换,共用一个调度数据网地址,建立与厂站端的104规约通信,成功解决了上述难题。通过在泉州电网调度控制系统改造过程中的应用证明了该技术的有效性。

1 NAT技术概要

NAT是将IP数据报头中的IP地址转换为另一个IP地址的过程。在实际应用中,NAT主要用于实现私有网络访问公共网络的功能。通过使用少量的公网IP地址代表较多的私网IP地址的方式^[1]。NAT技术应用的初衷是为了缓解互联网IP地址的枯竭。NAT地址转换基本过程如图1所示。

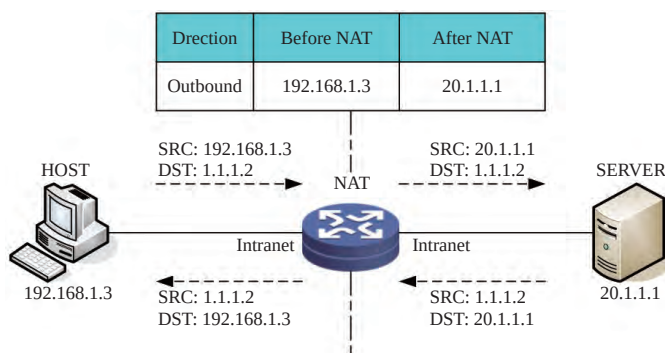


图1 NAT地址转换基本过程

关键词/Keywords

调度控制系统·
网络地址转换·
端口镜像·
端口地址转换·
监听前置服务·

内网用户主机PC (192.168.1.3) 向外网服务器 (1.1.1.2) 发送的IP报文通过NAT设备: NAT设备查看报头内容, 发现该报文是发往外网的, 将其源IP地址字段的私网地址192.168.1.3转换成一个可在Internet上选路的公网地址20.1.1.1, 并将该报文发送给外网服务器, 同时在NAT设备的网络地址转换表中记录这一映射; 外网服务器给内网用户发送的应答报文 (其初始目的IP地址为20.1.1.1) 到达NAT设备后, NAT设备再次查看报头内容, 然后查找当前网络地址转换表的记录, 用内网私有地址192.168.1.3替换初始的目的IP地址。

2 NAT技术在调度控制系统改造中的应用

2.1 技术适用性分析

调度控制系统的改造需要经历一定的时间, 在此期间新旧两套调控系统必须能够并列运行, 并且能够满足对新系统进行厂站远动信息接入调试的要求。如前所述, 希望能找到一种技术来实现在不增加厂站端远动104规约链路的情况下将厂站远动信息同时接入新旧两套调度控制系统。显然, 如不增加厂站端远动104规约链路, 则意味着新旧两套调控系统的前置数据通信服务器必须要能实现共用一套调度数据网IP地址。而NAT技术本身就能够解决多个内部网络主机共用一个外部网络地址的问题, 因此采用NAT技术来实现新旧两套调控系统共用一套前置服务器调度数据网IP地址的方案。在此方案中, 可将新旧两套调控系统的前置服务器分别通过交换机与NAT路由器和调度数据网连接, 新旧系统的前置服务器分别用于各自的私网 (调控系统局域网) IP地址, 经NAT路由器的地址转换后, 将拥有同样的公网 (调度数据网) IP地址。

2.2 NAT技术应用于调度控制系统改造需要解决的若干问题

1) 由于厂站端远动机仅通过注册IP地址来识别与之建立104规约通信的调度主站, 因此同时只有一套调控系统与厂站端远动机建立104规约通信, 否则将会引发规约通信混乱。

2) 由于厂站远动信息需要同时接入新旧两套调控系统, 但同时又只能有一套系统与厂站端远动机建立104规约通信, 因此需要解决其中一套系统建立与厂站104规约通信的同时, 在另一套上系统如何接收厂站远动信息的问题, 否则将无法满足不同两套调控系统并列运行的要求。

3) 由于新旧两套调控系统同时只能有一套系统来发起建立与厂站端的104规约通信, 因此两套系统都必须解决是否由其来发起建立104规约通信的问题。

2.3 NAT技术应用于调度控制系统改造的具体实施方案

针对前文提出的三个问题, 给出如下的解决方案。

(1) 交换机端口镜像技术的应用

交换机端口镜像技术是通过在交换机上创建一个镜像组, 将一个或多个源端口的数据流量转发到某一个指定端口来实现对网络的监听, 指定端口称之为镜像端口或目的端口^[2]。如果将新旧两套调控系统的前置数据通信服务器连接到同一台交换机上, 然后在交换机上创建一个镜像组, 使其包含新旧两套系统前置服务器所连接的交换机端口, 如以旧系统前置服务器所连接的端口为被监听端口, 以新系统前置服务器所连接的端口为镜像端口 (监听端口), 则当旧系统发起建立与厂站端104规约通信时, 新系统前置服务器所连接的端口上即可接收到同样的IP报文, 这就为新系统同时接收厂站端远动信息创造了条件。

(2) 旁听104规约的应用

如上所述, 采用交换机端口镜像技术解决了主子站报文的监听, 但系统同时还必须提供对规约报文的解析功能, 此时常规的104规约程序显然无法解决该问题, 常规104规约程序必须建立在主子站信息交互的基础上, 调度自动化主站作为规约通信的客户端, 主动发起与作为规约通信服务端的厂站远动机 (调度自动化子站) 的104连接, 在此基础上进行主子站信息交互。为此, 采用旁听104规约程序来解决此问题, 旁听104规约程

序从交换机镜像端口上接收来自被监听端口的报文，剥离其网络层和传输层报头，仅保留其应用层服务数据单元，即104规约所定义的应用服务数据单元（ASDU），即可对报文中所包含应用层信息进行解析，从而获得厂站上传的实时信息。

（3）路由器NAT配置

NAT连接示意图如图2所示，新旧两套调控系统的前置数据通信服务器分别为CCS-NEW-01A/172.20.10.9、CCS-OLD-01A/172.20.10.1，两台服务通过交换机与NAT路由器互连，其与调度数据网的互连接口为G 0/0/0，NAT配置分为以下三个步骤。

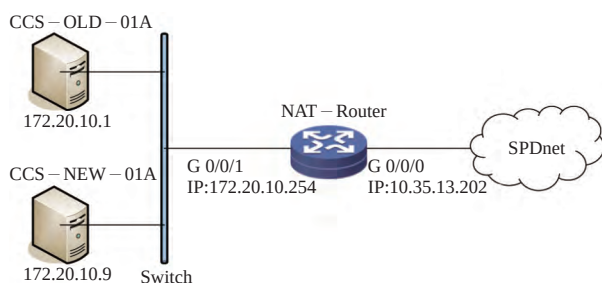


图2 NAT连接示意图

1) 首先配置访问控制列表

```
[NAT-Router]acl number 2000
```

```
[NAT-Router-acl-basic-2000]rule permit  
source 172.20.10.1 0
```

```
[NAT-Router-acl-basic-2000]rule permit  
source 172.20.10.9 0
```

2) 然后再配置NAT地址池

```
[NAT-Router]nat address-group 1 10.35.13.1  
10.35.13.1
```

3) 最后将访问控制列表和NAT地址池应用于G 0/0/0接口

```
[NAT-Router]interface GigabitEthernet 0/0/0  
[NAT-Router-GigabitEthernet0/0/0]ip  
address 10.35.13.202 255.255.255.0
```

```
[NAT-Router]nat outbound 2000 address-group 1
```

以上配置中NAT地址池仅包含一个用于转换的公网地址（调度数据网地址），且NAT配置中

未启用端口地址转换（PAT），确保了同时只能有一台内网主机（CCS-NEW-01A或CCS-OLD-01A）发起对外部网络的访问。

（4）增加监听前置服务组

如前面所述，厂站远动信息同时被新旧两套调控系统接收，其中一套系统主动发起并建立与厂站端的104规约通信，而另一套系统则采用交换机端口镜像技术，实现对前者收发报文的监听，并采用旁听104规约对报文进行解析。新旧两套系统都必须解决是否由本系统来发起并建立与厂站端104规约通信的问题。对此，本文采用了在新旧两套系统中各自增加一组监听前置服务的方法，建立如下的前置通信模型，模型中包括厂站、RTU、通道和前置服务组四个基本元素，厂站与RTU（表示厂站端的远动机）、RTU与通道以及通道与前置服务组分别建立关联，厂站实时信息来自RTU，RTU可选择其工作通道，而通道可选择其工作在哪个前置服务组上。当在系统中增加一个监听前置服务组后，无须改变通道参数配置，通过切换其工作的前置服务组，就可确定其所在系统是否主动发起建立与厂站端的104规约通信；当通道工作在正常的前置服务组时，其所在的系统就主动发起并建立与厂站端的104规约通信；当通道切换到监听前置服务组工作时，其所在系统就选择被动监听另一套系统与厂站端的104规约通信报文，如此一来就很好地解决了前面所提出的问题。

图3为上述新增监听前置服务组的示意图。图中，CCS-NEW-01A、CCS-OLD-01A分别为新旧两套系统的前置数据通信服务器，两台服务均有两个网络接口引至NAT交换机，其中一个网络接口为正常的104规约通信业务端口，另外一个为104规约通信业务监听端口，与CCS-NEW-01A的端口1和CCS-OLD-01A的端口2互连的交换机端口建立交换机镜像组，与CCS-OLD-01A的端口1和CCS-NEW-01A的端口2互连的交换机端口建立交换机镜像组，这样便可以实现新旧两套调控系统104业务报文的相互监听。

（5）PAT（Port Address Translation，端口地址

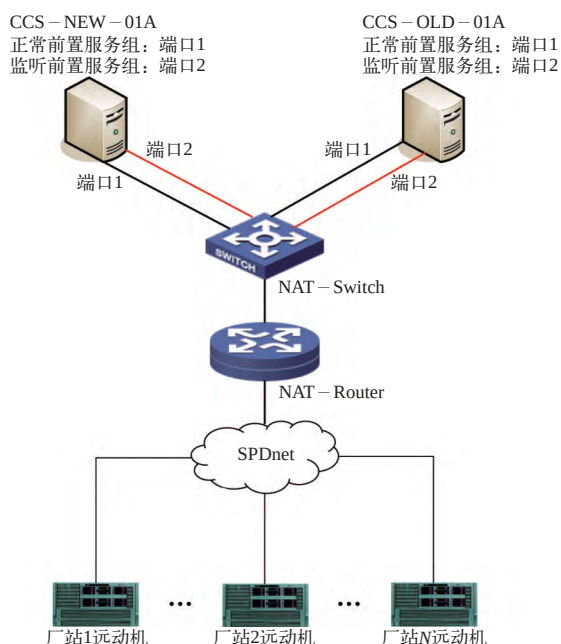


图3 新增监听前置服务组的示意图

转换)技术的应用

2.2节问题2)、3)针对的是本地调控系统主动发起并建立与厂站端的104规约通信,此时调控系统作为104规约通信的客户端,厂站端的远动机作为规约通信的服务端;但是当本地调控系统作为104规约通信的服务端向其他调度机构的调控系统转发数据时,104规约通信由外部系统来主动发起,此时简单的NAT地址转换就无法满足要求了。

仍以图2为例说明,无论由新旧哪套调控系统来主动发起与厂站端的104规约通信,当104规约报文穿越NAT路由器时,将其源IP地址字段的私网地址172.20.10.1或者172.20.10.9都将被转换为NAT地址池中设置的公网地址10.35.13.1,与此同时在NAT路由器的网络地址转换表中将记录这一映射;当厂站端远动机向调控系统回送的应答报文到达NAT路由器后,路由器再次查看IP报头内容,然后查找当前网络地址转换表中的记录,用内部网络私有地址172.20.10.1或者172.20.10.9替换目的IP地址10.35.13.1,这样调控系统与厂站端远动机便可以进行正常的104规约报文交互。但是当本地调控系统自身作为服务端向其他调度机构的调控系统转发数据时(比如地调系统向省调系统转发数据),104规约通信的发起方是来自外部网络的调

控系统,在这种情况下,当发起方的报文到达本端系统NAT路由器时,NAT路由器将无法确定应该将此报文转发给哪一套系统的前置数据通信服务器。由此可见简单的地址转换已然无法满足要求。因此在本文中采用静态PAT技术来解决这个问题。

PAT技术是NAT的一种变形,当IP报文在穿越NAT设备时,同时对源IP地址源端口进行转换,它允许不同的内部网络主机并发访问外部网络,采用不同的转换端口来区分不同的内部网络主机与外部网络之间的会话,这样当外部网络回送应答报文时,就不会造成NAT设备报文分发的混乱^[3]。PAT分为静态PAT和动态PAT两种,由于104规约通信端口恒定为2404端口,因此本文选择采用静态PAT技术,通过在NAT路由器上建立IP地址+端口“一对一”映射关系来解决外部系统报文转发问题,在前文描述的配置基础上增加如下的配置:

```
[NAT-Router]nat server protocol icmp global
10.35.13.1 inside 172.20.10.1
```

```
[NAT-Router]nat server protocol tcp global
10.35.13.1 2404 inside 172.20.10.1 2404
```

第一条用于ping命令测试网络的连通性,第二条则用于外部系统应答报文的转发。由命令配置可知外部调控系统发送的目的地址10.35.13.1,端口2404的IP报文将被转发至内部网络上目的地址172.20.10.1,端口2404的应用,即旧系统的前置服务程序。如此本地调控系统就能向外部调度机构的调控系统正常转发数据。该案例中将数据转发配置在旧系统上,当需要测试新系统对外部调控系统的转发功能时,可将配置修改如下:

```
[NAT-Router]nat server protocol icmp global
10.35.13.1 inside 172.20.10.9
```

```
[NAT-Router]nat server protocol tcp global
10.35.13.1 2404 inside 172.20.10.9 2404
```

(6) 路由配置

改造后的调控系统,其前置数据通信服务器不再直接接入调度数据网,而是经由NAT路由器与调度数据网的接入交换机连接,因此必须修改前置服务器上的路由配置,仍以图2为例说

明如下：若设调度数据网路由器上网关设置为10.35.13.254，NAT路由器与NAT交换机连接的接口G 0/0/1的IP为172.20.10.254，则必须将新旧两套调控系统上前置服务器的网关地址均设置为172.20.10.254，这样出口的报文将被直接发往G 0/0/1接口。但仅仅如此还不够，来自本地调控系统的104规约报文出NAT路由器后必须发至调度数据网的网关，因为只有这样报文才能被最终送达至目的主机接收，必须考虑在NAT路由器上增加路由配置，为此选择在NAT路由器上进行静态路由配置，设35.13.161.0/24、35.13.162.0/24、35.13.163.0/24均为厂站端远动业务对应的网段，10.35.0.0/16为外部调控系统对应的业务网段，配置命令如下：

```
[NAT-Router]ip route-static 10.35.0.0
255.255.0.0 10.35.13.254 preference 60
```

```
[NAT-Router]ip route-static 35.161.0.0
255.255.0.0 10.35.13.254 preference 60
```

```
[NAT-Router]ip route-static 35.162.0.0
255.255.0.0 10.35.13.254 preference 60
```

```
[NAT-Router]ip route-static 35.163.0.0
255.255.0.0 10.35.13.254 preference 60
```

做上述的路由配置，无论是去往网厂站端远动机还是去往外部调控系统的104规约业务报文都会被指向调度数据网的网关10.35.13.254，这样也就保证报文最终被送达至目的端的业务主机。

3 实际工程应用

通过实现NAT技术在调度控制系统改造中的应用，可以很好地解决厂站端新增104规约链路的问题，在确保接入数据正确可靠的基础上极大地缩短改造工期，提高厂站远动信息接入调试工作效率，其在泉州供电公司调度控制系统改造工程中的应用进一步验证了该技术的可行性和有效性。

泉州供电公司调度控制系统于2016年立项进行改造，2017年启动厂站接入调试工作，地调管辖范围内110 kV及以上厂站共计约有250座，若按常规作业，为每座变电站的双套远动机分别增加104规约通信链路，即使不考虑部分厂站已无法再

新增链路的因素，整个厂站远动信息接入调试工作，时间跨度也需要近1年，工程量十分庞大，加之工程进度要求紧迫，基于这样的状况，泉州地调经过慎重考虑，决定应用NAT技术来提升改造工作效率。

3.1 改造前的系统基本情况

泉州地调原有的地区电网调控系统采用积成电子iES600调控一体化系统，系统共部署两组前置服务器，每组前置服务器由两台前置服务器组成，两组前置服务器分别处理常规四遥远动信息和厂站微机保护报文信息，每台前置服务器分别接入调度数据网（SPDnet）骨干网一平面和骨干网二平面^[4]，实现与调度管辖范围内的各厂站及省调D5000系统进行104规约通信。各前置服务器IP地址分配情况如表1所示。

表1 旧系统前置服务器调度数据网IP地址分配表

前置服务器组	常规四遥前置服务器组		厂站微机保护前置服务器组	
前置服务器	600CCS01A	600CCS01B	600CCS02A	600CCS02B
骨干网一平面	10.35.13.1	10.35.13.2	10.35.13.3	10.35.13.4
骨干网二平面	35.13.10.1	35.13.10.2	35.13.10.3	35.13.10.4

3.2 改造后的系统基本情况

改造后的系统采用积成电子新一代地区电网调控iES700系统，新一代系统对前置服务进行了优化，通过设置两个前置服务进程，可实现在一台前置服务器上同时接收处理常规四遥信息和厂站微机保护信息，这样新系统只需配置两台服务器，系统改造过渡期间新旧两套系统并列运行，为此考虑采用NAT技术对两套系统的前置部分进行重组，分别为新旧两套系统共计六台前置服务器分配私网IP，形成八个NAT组合。考虑对实时数据传输实时性的要求，NAT路由器选用H3C AR4640路由器，NAT接入交换机使用H3C S5500交换机，详细的分组及地址分配情况如表2所示。

考虑到每台AR4640路由器最多能承载两个NAT分组，因此改造过程中共设置了四台路由器和四台交换机，每一台路由、一台交换设备承载两个NAT分组。同时为了保证新、旧两套调控系统能同时接收厂站端远动信息，在每台交换机上配置

表2 过渡系统NAT分组及前置服务器私网IP地址分配

NAT组别	600系统		700系统		公网IP	所属网络
	前置服务器	私网IP	前置服务器	私网IP		
1	600CCS01A	172.20.10.1	700CCS01A	172.20.10.9	10.35.13.1	骨干网一平面
2	600CCS01A	172.20.20.9	700CCS01A	172.20.20.9	35.13.10.1	骨干网二平面
3	600CCS01B	172.20.10.3	700CCS02A	172.20.10.13	10.35.13.2	骨干网一平面
4	600CCS01B	172.20.20.3	700CCS02A	172.20.20.13	35.13.10.2	骨干网二平面
5	600CCS02A	172.20.30.7	700CCS01A	172.20.30.5	10.35.13.3	骨干网一平面
6	600CCS02A	172.20.40.7	700CCS01A	172.20.40.5	35.13.10.3	骨干网二平面
7	600CCS02B	172.20.30.8	700CCS02A	172.20.30.6	10.35.13.4	骨干网一平面
8	600CCS02B	172.20.40.8	700CCS02A	172.20.40.6	35.13.10.4	骨干网二平面

了四个端口镜像组，实现两两监听。

4 结束语

本文系统地阐述了NAT技术应用于电网调度控制系统改造过程中厂站远动信息接入调试的实现方案，该方案以NAT技术为主要特征，综合运用了包括交换机端口镜像、旁听104规约、监听前置服务以及PAT等多种技术，实现了各种技术的完美衔接组合，在不改变各厂站端远动机配置且不对旧系统实时数据造成影响的情况下，完成新系统厂站远动信息接入调试，极大地缩短了厂站远动信息接入调试的周期，显著提高了整个新一代系统的建设工作效率，且在新系统功能完全调试完毕后，只需做很少的改动即可实现新系统切主运行和旧系统退出。对于国内其他电网调度机构技术支持系统改造提供了很好的借鉴，具有很好的推广价值。当然，该技术也还存在一些问题：

1) 由于NAT路由器承载能力的限制，造成改造过程需要配置为数较多的网络设备，对系统环境资源造成较大压力，除空间占用外，还造成系统用电负荷较大的攀升。

2) 测试新系统对厂站远动信息接收处理功能时，需要在新旧两套系统上先后进行操作，首先在旧系统上将厂站通道切换到监听前置服务组，启用监听模式接收厂站远动信息，然后在新系统上将同一厂站的同一通道切换到正常前置服务组，启用正常的104规约通信模式接收厂站远动信息，切换操作要求顺序不能乱、连续完整且必须在尽可

能短的时间内完成，存在因人为失误造成厂站实时信息丢失，甚至引发规约通信混乱的隐患。

3) NAT路由器和交换机的性能是技术成败的关键，特别是NAT路由器，对其报文转换处理的性能要求较高。以泉州电网为例，目前虽然在电网正常运行情况下，数据实时性能满足调度监控的要求，但尚未经历较大故障和恶劣天气条件的考验，在恶劣条件下，网络中的报文数量将呈现出激增的状况，NAT路由器的处理性能尚需要做进一步验证。

针对上述问题，一是必须采取暂时将系统中一些次要的或是不必实时在线运行的应用暂时退出的措施，以减轻供电负荷压力；二是通过制定厂站通道切换作业指导书完善作业过程管理，以降低操作风险；三是必须在工厂测试阶段开展系统雪崩试验，对NAT路由器和交换机的性能进行充分的仿真评估。

参考文献

[1] Nader F Mir. 计算机与通信网络 [M]. 北京：中国电力出版社，2010。
[2] 韩旭. 自动化远程维护实践 [J]. 电气应用，2015 (增刊2)：433-436。
[3] 吴建军，周伦钢. NAT模式下的VPN使用 [J]. 华北水利水电学院学报，2004，25 (3)：62-64。
[4] Q/GDW 11407—2013 国家电网调度数据网应用接入规范 [S].

(收稿日期：2016-11-01) EA