Definity-G(x) Demystified:
By Walt Medak

Q. I have been given the task to block all remote access our Definity G3si and allow access only on an as needed basis. I understand that my Remote Monitoring group will not be able to monitor and respond to server alarms. How do you suggest I handle this? Is it possible to have two lines; one for the server to send out alarm notification and another for remote access?

Thank you
Peggy Tatum

A. Thank you, Peggy, for the good question. It made me stop to think about the separation of inward-versus-outward in terms of an "INADS" line (what you are calling Remote Access). Remote Access is actually the ability to dial into your system and place a call back out on the PBX's lines. Often it's used for people who are not always in the office so they don't need to use a calling card or charge the call to their personal phone. I had never considered it before, but since you asked, there actually is a way to connect a line for the PBX to dial out and report problems, yet not allow incoming calls. This could be accomplished by connecting the port of an analog station to the INADS termination. In that it's one of your analog stations, you could then give it a COR that didn't allow the calling of that analog station by changing the "Called Party Restriction" field from "none" to one of the choices that doesn't allow a call to terminate to that station such as "inward" or "termination". There is also another option called "public", but I'm not sure of it's operation; I will assume it will allow calls from inside the system to ring there, but not calls from outside the system. If that is indeed the case, that may be a good option as it would allow you to dial into the system from your workstation but not allow anybody to dial in from the outside. If the analog line was given one of your DID numbers, upon your changing the COR's "Called Party Restriction" field, you could alternately deny or allow calls to access the switch for your maintenance company at your discretion.

Now, after going through all of that, I would not recommend restricting a PBX from either calling out or being called, as it limits the ability of your maintenance company from assisting you in keeping the system functional. If it calls out, as in the above example, and your maintenance company can't dial back into it to determine the extent of the problem, you will have two problems. One is that the maintenance company may ask you to not have it call them any more if they aren't allowed the ability to remotely fix the problem to either repair it or notify the system they have received the report so the system will stop it's incessant re-dialing to them (the system will repetitively call every seven to twenty minutes until it's given a command to cease). This can be very disruptive and frustrating to the maintenance company. The second is that there may be a fault or problem that occurs out-of-hours that you could have repaired before the next business day, or at least at the beginning of the business day instead of having to wait for the system to be connected for them by you, after you get there in the morning, so that they can call into it.

There is a much simpler method that takes care of both your concerns and the concerns of the maintenance company. It's the installation of the Definity RPSD (Remote Port Security Device). It is comprised of two compatible units; one is the Lock and the other is the Key. The Lock is installed on the INADS line ahead of the Definity, and any call into it that's not through the Key device that has been programmed to specifically the identical code as the Lock will be denied access into the system. It just hangs up on the call. We use it on our system and have great confidence in it.

If you have a software release of V6 or higher, you also have a built- in security system called ASG (Access Security Gateway) that upon typing in the login, such as "craft" will present the caller with a "challenge" number of seven digits. The caller must then provide the system with a

"response" of seven different digits that have been screened through a "Key" and are the only seven digits that the system will identify. It is extremely difficult, if even possible to hack into a system that uses either of these two security methods. And then, if one is really concerned, there is the possibility of using both systems, which would just about reduce the security exposure from any concern whatsoever.

At any rate, Peggy, you have several options that make more sense than to isolate your system from the maintenance support it should be getting. If you have any questions about the security information above, please feel free to call me.

Thanks again for the query, Peggy.