



Why RADIUS and TACACS+ both fail to protect remote technician dial up access to the router/server

Today most router products on the market provide a console/maintenance port for direct access to a router/server's functions. Typically, this port is connected to a network terminal server or a dial-up modem, allowing the technician on call convenient remote access when network problems arise.

When a network issue does occur, the technician can select one of several options, depending on how his network's topological and geographic configuration:

- In a **simple network**, the technician may be close enough to the router/server, allowing him to physically connect to the console/maintenance port, perform diagnostic tests, and resolve the issue.
- In a more **diverse and complex network**, there are a greater number of options available. Each has its own distinct set of consequences.

Let us assume that the technician and the router are not located near one other. For the sake of this scenario, we should imagine that they are situated in distant cities. When a network problem occurs, the technician can deploy one of eight options – six of which demonstrate network vulnerabilities:

1. Multiple Staff Members at All Locations

The technician can try to contact staff members at the remote site and work with them to diagnose the problem over the telephone. This option presupposes that the company has employees with similar (though possibly less advanced) skills and tools as the technician, at each of its remote sites.

2. Technician On-Site Visits

The technician can physically travel to the site by car, train, or plane. This option is costly and time consuming, and incurs travel and possibly hotel expenses. In addition, the primary site has to cope with the loss of the technician's services while he is away.

3. Network Terminal Server

A network terminal server can provide serial access to the console port of the remote router. However, you need the network functioning properly to use the terminal server. Therefore it is not feasible to use a network terminal server to fix a broken network. If you manage to access the terminal server, it will use the network to attempt to secure your access. The problem is, as noted earlier, you cannot use a broken network to secure itself.



4. Unsecured Dial-Up Modem

A dial-up modem can be placed on the console/maintenance port of the router that the technician can use to dial into the router whenever necessary. While this solves the problem of being able to remotely diagnose the problem, it creates a significant security violation. Now anyone who has the ability to dial in can access the router/server, thereby circumventing any security or audit restrictions.

5. Turning On and Off an Unsecured Dial Up Modem

To address the potential security exposure, the technician can ask that someone at the remote site turn the modem on only when a problem occurs, and then have them switch it off as soon as the issue is resolved. This requires that someone be available at the remote site 24 hours a day, seven days a week.

If availability is not a concern, there is the possibility that someone might forget to turn off the modem accidentally. Or, in an even more dire scenario, they might purposely leave the modem on because they themselves wish to connect to the network after hours, knowing that they will be undetected by the global security system. In short, simply switching the modem on and off still leaves the system open to attack.

6. RADIUS or TACACS+ Authentication

The technician can use a RADIUS or TACACS+ authentication server to authenticate the dial-up call securely with a remote two-factor authentication token. This is a great idea in theory – and as such, is utilized by many organizations – but in practice it still exposes the network.

Using the RADIUS or TACACS+ protocol requires Internet connectivity. If the router/server is connected to the network via the Internet, many technicians will opt to use the network to access the router/server rather than the dial line.

If the router/server does not have network connectivity, the technician will be forced to use dial access to the console/maintenance port. However, once the network is down, so too is RADIUS/TACACS+ authentication. So these protocols are not available to provide secure authentication into the console/maintenance port. Potentially, this is an enormous security breach.



7. Password-Protected Modems

The technician can install password-protected modems at every remote site that requires dial up access. This resolves his remote access issues, but creates two additional challenges:

- a. Password authentication is easily thwarted. To be truly secure, two-factor authentication should be incorporated into a strong authentication modem – which is not a commonly available product.
- b. Because there may be hundreds of individual databases scattered throughout the network, security personnel may find these schema difficult to manage. Any updates to these databases will be labor intensive, as will providing audit information, if available.

8. Strong Authentication Modems, Centrally Managed Database

The only totally secure and manageable remote access solution is to install strong authentication modems with a built-in, centrally managed database. This eliminates the need to secure network connectivity that is only used during network problems and outages.

A centrally managed modem allows a single management station to control access to thousands of router ports, ensuring the highest level of authentication for each access attempt. This central manager, which can connect both via network and via dial line if the network is down, can also provide daily audit reports from each modem, including a detailed list of all events on the modem.

Summary

RADIUS and TACACS+ do not address the challenges associated with remote technician access to router/server ports. This problem can only be adequately addressed by centrally managed, secure access modems with strong authentication.

This paper is provided by Communication Devices Inc., a supplier of secure network communications for more than a decade. CDI manufactures a complete line of Secure Out of Band Management solutions including the UniGuard and Port Authority products lines which are capable of being centrally managed by CDI's Distributed database Manager. More information can be found at www.outofbandmanagement.com