Backhaul Research Note:

FIPS Certified Backhaul Equipment

Maravedis-Rethink

December 2013

What does *secure* backhaul mean?

Customer privacy has always been a concern for telecom service providers. However, the popularization of packet-based network technologies has forced operators to pay attention to security, as anyone can gain access to equipment that could illegally intercept communications. Although security requirements can be analyzed at each of the components of a communications network (base station, end-user terminal, core network…), as part of the backhaul service this research note focuses on transmission networks between the RAN (Radio Access Network) and the core network.

There are different levels of security depending on the kind of threats that are considered. The first parameter to monitor is **link security**, which is ensured by data encryption mechanisms such as AES (Advanced Encryption Standard). It is interesting to note that wireline backhaul connections can also suffer security issues, since they can be accidentally or intentionally broken. The most typical example of the first case is damage during civil works, while another common cause is theft, related to the value of copper in the black market.

Physical security is related to the capability of any malicious individual to access the cell site equipment physically. Security concern is particularly high for metrocells, since they are deployed in public spaces, at lower heights than macrocells and lacking any kind of fenced shelter or video surveillance protection. Such vulnerability makes it easy to access backhaul Ethernet connectors to monitor the traffic. For this reason the encryption mentioned above should be applied not only to each link or port, but also to the information that is kept in the backhaul device.

Since backhaul equipment supports remote configuration through different protocols, backhaul **security threats can be also remotely generated**. It is important that unsecure protocols such as Telnet and FTP (File Transfer Protocol) are replaced by secure alternatives such as SSH (Secure Shell) and sFTP (Secure FTP). In the case of providing a remote web-based configuration interface, HTTPS (Secure HTTP) should be used. Security in automated network management based on SNMP (Simple Network Management Protocol) needs also to be enforced by using version 3, which adds security support to previous versions of the protocol. In order to provide an additional tool to protect the network, it is important to implement a centralized authorization and authentication server (with RADIUS for example) to control all the users who have access to network

Backhaul Research Service

This note is part of the backhaul research service and is not available for sale individually. Led by Esteban Monturus, the Backhaul service covers the whole backhaul industry with a special focus on small cells and wireless technologies, including PTP, PMP, sub-6 GHz and other emerging technologies. In order to provide the complete backhaul picture, the service also analyzes wireline and networking trends such as the TDM-to packet evolution and the adoption of MPLS. The service provides in-depth backhaul vendor profiles & SWOT.

Analysis as well as carrier expectations & trends. Annual subscription includes two comprehensive reports and 18 research notes on important industry developments as well as analyst support.

About the author:

With over ten years of experience in the wireless industry, Esteban Monturus holds an MSc degree in Telecommunications Engineering from the University of Zaragoza (Spain) and is following an Executive MBA in IESE Business School (Barcelona, Spain). He started his professional career at the R&D Department of Teltronic SAU, one of the leading professional radio communications equipment manufacturers in the world. For five years, Esteban developed and tested wireless broadband equipment, including Bluetooth, WLAN and especially Mobile WiMAX. Technical and analytical skills acquired at Teltronic allowed him to join Maravedis as market analyst for 4G operators and backhaul. During this stage, he contributed to 4GCounts service in Europe and authored several research reports on mobile backhaul. In 2011, Esteban decided to start an IT services business targeted at SMEs in Spain. Taking advantage of such a great experience, he is now back at his analyst position, now fully focused on mobile backhaul, one of the hottest topics in the mobile industry.