This Reference Guide addresses WiFi and Internet Security considerations using the Mintaka STAR and Mintaka STAR**X/XG** in the NOAA/NWS VOS Program.

Introduction

The Mintaka STAR in conjunction with the Mintaka STAR**X** or STAR**XG** introduce a WiFi capability to the Mintaka line of electronic weather instruments. The WiFi functions allow the STAR to connect to existing WiFi networks (which we call station mode) or to create it's own WiFi network (which we call access point mode). This WiFi capability is used when the STAR**X/XG** communicates observation data to the STAR. This is the primary use of WiFi within the context of the NOAA/NWS VOS program.

This document will outline the various scenarios in which the Mintaka instruments can be used in the NOAA/NWS VOS program and the WiFi/Internet security implications.

Scenario 1: Mintaka STAR and STARX/XG in Weather Service Mode

The most common way the STAR and STAR**X** or STAR**XG** are used is in Weather Service mode. In this mode the Mintaka STAR functions as a WiFi Access Point and hosts a WiFi network with name (SSID) of MintakaWX. The password is predefined as well but is only known by NOAA/NWS VOS personnel and the Mintaka Innovations staff.

The operation of the devices in this scenario are described below.

- When the Mintaka STAR is powered up it creates a WiFi network with the name MintakaWx and with a predefined password.
- When TurboWin+ (TW+) launches, it looks for a STAR on a COM port and when it finds one, it programs the STAR to send reports in the appropriate format (based on settings in TW+) over the COM port every minute.
- When the Mintaka STAR**X/XG** is initially powered up, or when it wakes from sleep, it collects data for a weather observation.
- When the STAR**X/XG** is ready to communicate the observation data, it connects to the predefined WiFi network MintakaWx with the password.
- After connecting to the STAR WiFi network the STAR**X/XG** opens a TCP connection and sends the data to the STAR. (Since the STAR is hosting the WiFi network the STAR**X/XG** knows the IP address of the STAR.)
- After the STAR**X/XG** completes its report it closes the TCP connection, disconnects from the WiFi network and goes to sleep, usually for 5 minutes. At the NOAA/NWS VOS PMO defined time interval, the STAR**X/XG** wakes up and repeats the above process.
- When the STAR receives the report from the STAR**X/XG** it stores it internally. Every minute the STAR formats the report appropriately and forwards it on to TW+ over a USB connection operating as a COM port. Thus the transfer of the report is initiated by the STAR.

In this scenario the Mintaka STAR and STAR**X/XG** operate their WiFi network as a WiFi Island. They are not connected to any other network and are not connected to the Internet, so there is no risk to the network infrastructure of a hosting ship.

If someone were to discover the password of the STAR network, they could connect to the network using a PC, phone or tablet - this is often done by PMO's in order to trouble shoot and verify proper operation of the system - however, since the network is a WiFi Island, any actions they take cannot impact the hosting ship's network infrastructure.

Scenario 2: Existing WiFi Network with STAR and STARX/XG Operating in Station Mode

In this scenario, an exiting WiFi network is hosted by another device (i.e., a hosted network, typically a WiFi router) and the STAR and STAR**X/XG** use this network. I do not believe that any NOAA/NWS installations use this capability. This scenario is included solely for reference guide completeness.

The operation of the devices in this scenario are described below.

- When the STAR is powered up, it connects to the hosted network using a preassigned network name and password. The network name and password are stored inside the STAR during installation. The password is never accessible or exposed. The STAR is connected to a PC running TW+ via USB/COM port as in Scenario 1.
- When the STAR**X/XG** is powered up, or wakes from sleep, it connects to the same hosted network using the preassigned network name and password. As with the STAR the network credentials are stored inside the STAR**X/XG** and the password is not exposed or accessible.
- When the STAR**X/XG** is ready to send a weather observation it connects to the STAR and sends the report as in Scenario 1. In this case however the STAR**X/XG** is configured ahead of time with the IP address of the STAR on the hosted WiFi network.
- In other respects this scenario is the same as in Scenario 1.

Note that in this scenario, the hosted network is only used to transfer data between the STAR and the STAR**X/XG**. Neither devices knows the IP address of the networks router because it uses no networking infrastructure such as DNS (Domain Name System) and no routing services in order to access other network devices. The STAR and STAR**X/XG** operate as if they were running (as they may well be) on a WiFi Island. The STAR and STAR**X/XG** do rely on DHCP (dynamic host configuration protocol) to get assigned IP addresses.

Scenario 3: Using Mintaka ENet to Send Observations to TurboWin+

Normally the Mintaka STAR is connected to a PC where TurboWin+ (TW+) is running and data is transferred to TW+ over a USB cable. However, many ships are moving away from physical PCs on the bridge deck and using Virtual PCs. If this is the case there is no USB port available to connect the STAR to the Virtual PC that is running TW+.

The solution in this situation is to connect the Mintaka STAR to the ship's network infrastructure with a Mintaka ENet device, shown below.

In this case, the STAR is connected via its USB cable to the ENet, and the ENet is connected to the ship's network via an ethernet cable.

In this scenario the operations of the system is as described below.

- The communication between the STAR and the STAR**X/XG** is done as in Scenario 1. (It is possible to use Scenario 2 but this is never done.)
- When the STAR is ready to send a report to TW+ it sends it over the USB cable as it normally does.
- The ENet device reads the STAR report and in turn transmits it over its subnet using a UDP (user datagram protocol) broadcast. This broadcast only goes as far as its subnet.
- TW+ listens for this broadcast, and when it receives one, it processes it appropriately. Note: The ENet device and the virtual PC must be on the same subnet.

The security considerations around communication between the STAR and STAR**X/XG** are as in Scenario 1.

The ENet device is connected physically to a local subnet. This implies that it can be managed more directly within the network infrastructure by IT. For example, in a firewall IT can block any incoming or outgoing connection to/from the ENet device. The services that the ENet device uses are DHCP and UDP. It does not use DNS or TCP or any routing services.