TECHNICAL WHITE PAPER

Network Services on MultiVantage™ Port Network Interface Boards

Version: **1.1** Date: **January 10, 2003**

CID: **95933** Author: **Avaya Security Architecture Group**

Abstract

This paper focuses on the use and accessibility of the Telnet, FTP (File Transfer Protocol), SNMP (Simple Network Management Protocol), Ping, and Traceroute network services on the components of Avaya MultiVantage Software powered Solutions. Each of the network interface boards in the MultiVantage network architecture uses an embedded real-time operating system (RTOS). Various network services are integrated into these embedded systems and are under the control of the RTOS and are used for configuration or system support of the boards. In some cases, certain network services are used to upload or download firmware. In other instances, these services are used to provide diagnostic or maintenance information to developers. Ping and Traceroute are utilities (not services) that are used on these embedded systems and may also be a concern to our customers. These particular services are used for either diagnosing network problems or determining the availability of IP phones or other IP interfaces on the network.

No services or utilities are used on these embedded systems unless they are necessary. Each of the embedded systems listed above is addressed in detail in this paper relative to the aforementioned utilities and services. This paper discusses the protections in place that make the presence of these utilities and services a manageable necessity and not a security liability. The combination of architecture, reduced services and clients, and restrictive mechanisms provide Avaya customers with an overall offering that they may consider trusted and secure on their enterprise network.

1 Scope

This paper focuses on the use and accessibility of the Telnet, FTP, SNMP, Ping, and Traceroute network services on the TN799C & TN799DP CLAN (Customer Local Area Network) boards, the TN2302AP Media Processing/MedPro boards, the TN2312 IPSI (IP Server Interface) board, and the TN2501AP VAL (Voice Announcement over LAN) board. The information is presented in the context of security and addresses mechanisms that are put in place to restrict access and misuse of these services. This paper applies to the following firmware versions of these boards:

- TN799C (CLAN): v5 or higher
- TN799DP (CLAN): v3 or higher
- TN2312 (IPSI): all versions
- TN2302AP (Medpro/Prowler): all versions
- TN2501AP (VAL): all versions

2 Overview

Each of the network interface board in the MultiVantage network architecture uses an embedded real-time operating system (RTOS). Various network services are integrated into these embedded systems and are under the control of the RTOS and are used for configuration or system support of the boards. In some cases, certain network services are used to upload or download firmware. In other instances, these services are used to provide diagnostic or maintenance information to developers. As such, these network services may be enabled by default while others may be enabled only through control commands from the MultiVantage Software acting as the media controller.

Telnet and FTP network services are usually of concern to customers since these protocols disclose all traffic in the clear to the network. This information includes the username and password that was used to gain access to that particular service. Ping and Traceroute are utilities (not services) that are used on these embedded systems and may also be a concern to our customers. These particular services are used for either diagnosing network problems or determining the availability of IP phones or other IP interfaces on the network.

No services or utilities are used on this embedded system unless they are necessary. Each of the embedded systems listed above is addressed in detail relative to the aforementioned utilities and services. However, a summary of these services for each board is found in the following table (N/A = not installed or available):

Board	Telnet		FTP		Ping	Trace-route	SNMP Agent
	Client	Service	Client	Service			
TN799C (CLAN)	N/A	• Suspended Task. • Enabled via MultiVantage command • Inactivity Timeout	N/A	• Disabled Task • Enabled via MultiVantage command • Inactivity Timeout	Available	Available	Read-Only MIB
TN799DP (CLAN)	N/A	• Suspended Task. • Enabled via MultiVantage command • Inactivity Timeout	N/A	• Disabled Task • Enabled via MultiVantage command • Inactivity Timeout	Available	Available	Read-Only MIB

TN2312 (IPSI)	Available	Available	N/A	• Available • Disabled by default. • Inactivity Timeout.	Available	Available	N/A
TN2302AP (Medpro /Prowler)	N/A	• Available • Can be Disabled	N/A	• TFTP Available • Disabled by default. • Inactivity Timeout	Available	Available	N/A
TN2501AP (VAL)	N/A	N/A	N/A	• Available • Disabled by default. • Inactivity Timeout.	Available	Available	Read-Only MIB

3 TN799C and TN799DP CLAN Boards

The following section covers the TN799C and TN799DP boards in detail.

3.1 Telnet for TN799C and TN799DP (CLAN)

Telnet is used for configuration and debugging of the CLAN boards. By default, the Telnet service on CLAN is started when the board is booted but it is placed in a suspended state within the run queue of the embedded operating system. This means that although the Telnet service is in the run queue as a task, access to the Telnet service is prevented unless a proprietary and restricted proprietary message is sent from the Avaya Media Server to the CLAN board. CCMS messages "un-suspends" the Telnet service and specify the username and password for that particular Telnet session.

Once the Telnet service is taken out of the "suspended" mode of operation, it will automatically return to a "suspended" mode if there is no successful login within five minutes. However, if a successful login is made, the session will not automatically terminate even if no activity is occurring.

When the Telnet service has been successfully enabled and accessed, no other logins are allowed as only a single user is allowed to access the Telnet service at one time. Finally, any bad login such as a bad login name or password will cause the Telnet daemon to be immediately suspended.

No Telnet client resides on the CLAN board. This prevents an individual who has been able to Telnet "into" the CLAN board from using that as a "jump-off" point into the customers network.

3.2 FTP for TN799C and TN799DP (CLAN)

Similar to Telnet daemon, the FTP service is only accessible from the network interface and not from any internal busses of the port network. However, unlike the Telnet daemon, the FTP daemon is disabled by default and the FTP task is stopped unless it is enabled. FTP is not kept in a "suspended" mode.

To enable the FTP network service, proprietary Avaya coded message must be sent to the CLAN board. This message contains the username and password for that session. This not only enables the service, but also creates the internal file system for management of the files that are downloaded to the CLAN board. Files that are loaded onto the CLAN board are then available via the internal buss of the port network to load into other boards. During the time that the files need to be made available to the port boards, the FTP service is enabled to maintain the file system. However, the internal transfer of files across the buss use Avaya proprietary messages, not FTP messages.

Since the FTP service is activated by the media server and is only used during the process of loading firmware into boards of the system, the FTP daemon does not implement an inactivity timeout. The FTP service must be manually disabled when it is no longer needed. This is accomplished from a command on the SAT screen of the Avaya MultiVantage Software.

No FTP client is available on the CLAN board. This prevents a person from establishing an FTP connection from the CLAN board with another FTP server.

3.3 Ping for TN799C and TN799DP (CLAN)

The TN799C and TN799DP boards provide the Ping utility. This utility is used for debugging of network connectivity. In addition, this capability is needed to determine the availability of other IP-related interfaces on the network that MultiVantage Software may need for the software to perform correctly. Examples of diagnosis using Ping would be to determine the connectivity or availability of other TN799C/DP or TN2302AP boards.

3.4 Traceroute for TN799C and TN799DP (CLAN)

Debugging the location of IP Phones of gateways in the presence of routers or firewalls is best accomplished using the Traceroute utility. As such, the CLAN boards possess the Traceroute utility for this purpose.

3.5 SNMP for TN799C and TN799DP (CLAN)

The TN799C and TN799DP boards implement SNMP agents for network management. The MIB information is read-only which prevents unauthorized modification of the MIB data.

4 TN2312 IP Server Interface (IPSI) Boards

This section discusses the TN2312 IPSI board in detail.

4.1 Telnet on TN2312

A telnet service is currently required on the IPSI for manual administration of the IPSI (IP address, default gateway address, VLAN ID, QoS and Ethernet settings). The IPSI supports the Telnet service on standard TCP port 23 but only for connections that are physically made through its secondary services Ethernet port. When established, these Telnet accesses are directed to a command menu supporting a variety of admin tasks.

The IPSI also supports Telnet access to an OS-debugging shell over port 2312. This port is always available when accessed through the local services port. Telnet access to port 2312 through the control network interface (Ethernet) but only after a triple-DES-protected command has been sent by the MultiVantage Software through the “IPSI link.” This command enables Telnet on the control network's port 2312. Telnet access to port 2312 is disabled immediately after a session has closed the connection or after 5 minutes of inactivity.

A Telnet client is present on IPSI and is required for the IPSI. It was put there to replace the SAT interface on the G3r EPN's. This allows the technicians to plug their laptop into the IPSI's if they're not physically close to the S8700 servers and then Telnet to the servers for administration. The capability is limited to the network interface and cannot be used to cross the TDM buss. Without this capability, the technicians would either have to plug their laptop into the customer's network to access the S8700 Media Server or walk/drive back to the media server to gain access.

4.2 FTP on TN2312

An FTP service exists but is disabled by default. A command from the MultiVantage Software establishes a triple-DES-protected channel to the IPSI and through it sends a command that enables the FTP service. Once the FTP service is started, the MultiVantage Software initiates the client-side of the FTP protocol and then transfers a new firmware file to the IPSI. Once the transfer is complete, the FTP service is automatically disabled. A five-minute-timeout is enforced to guard against cases where the firmware download is started but terminated prematurely. When timeout occurs, the FTP service is disabled until a new command from the MultiVantage software enables it again.

When enabled, the FTP service of the IPSI board is only accessible from the network (Ethernet) interface of the IPSI and not from the TDM buss.

No FTP client exists on the TN2312.

4.3 Ping on TN2312
The TN2312 possesses the Ping utility for debugging purposes. It is restricted for use to the network interface and cannot be used to ping "across" the TDM buss.

4.4 Traceroute on TN2312
The TN2312 possesses the Traceroute utility for debugging purposes. It is restricted for use through the network interface and cannot be used to Traceroute "across" the TDM buss.

4.5 SNMP for TN2312
A SNMP agent is not implemented on the IPSI.

5 TN2302AP Medpro Boards
This section discusses the TN2302AP Media Processing (Medpro) boards in detail. Sometimes this board is referred to as the "Prowler" board.

5.1 Telnet on TN2302AP
The TN2302AP board enables a Telnet service that is accessible via the network interface. It is used for configuration and maintenance of the system and normally cannot be disabled. However, if customers would like to prevent unauthorized access, the Telnet service can be disabled but this requires that a technician log into the board. In addition, the service is only disabled until the next time the board is rebooted. For additional security, there is a 20-minute inactivity timeout. If no activity occurs during a Telnet for 20 minutes, the session is terminated.

No Telnet client exists on the TN2302AP board.

5.2 FTP on TN2302AP
No FTP service is used on the TN2302AP. However, a TFTP service is used to load files onto the TN2302AP board and is disabled by default. To enable this service, a command must be provided to the board via a Telnet session with the board. In addition, a five-minute inactivity timeout is enforced. When this time is exceeded without activity, the service is automatically disabled.

No FTP or TFTP client exists on the TN2302AP board.

5.3 Ping on TN2302AP
For debugging purposes, the Ping utility is available on the TN2302AP and restricted to the network interface. Additionally, the Ping utility can only be executed on the TN2302AP from the SAT terminal of MultiVantage Software.

5.4 Traceroute on TN2302AP
For debugging purposes, the Traceroute utility is available on the TN2302AP and restricted to the network interface. Additionally, the Traceroute utility can only be executed on the TN2302AP from the SAT terminal of MultiVantage Software.

5.5 SNMP for TN2302AP
The TN2302AP does not use an SNMP agent.

6 TN2501AP VAL Boards

This section discusses the TN2301AP board in detail. This is sometimes referred to as the "Voice Announcement over LAN" or VAL board.

6.1 Telnet on TN2501AP

The TN2501AP does not have a Telnet service and therefore is not accessible via Telnet. In addition, there is no Telnet client on the TN2501AP.

6.2 FTP on TN2501AP

The TN2501AP uses a FTP service in its design to receive firmware downloads as well as new announcements. This service is disabled by default. However, it can be enabled with a command from the MultiVantage service SAT screen where the login and password for accessing the FTP service are specified. Enabling this service from the SAT screen sends a proprietary and restricted message from the MultiVantage Software running on the media server to the TN2501AP. This command enables the FTP service, which is accessible only via the Ethernet network interface and not from the TDM buss.

Once the FTP service is started, a 10-minute inactivity timeout is imposed. If no activity occurs for 10 minutes, the FTP service is disabled.

There is no FTP client on the TN2501AP.

6.3 Ping on TN2501AP

For debugging purposes, the Ping utility is available on the TN2501AP. However, it is only executable from the SAT terminal of MultiVantage Software.

6.4 Traceroute on TN2501AP

For debugging purposes, the Traceroute utility is available on the TN2501AP. However, it is only executable from the SAT terminal of MultiVantage Software.

6.5 SNMP for TN2501AP

The TN2501AP board implements an SNMP agent for network management. The MIB information is read-only which prevents unauthorized modification of the MIB data.

7 Summary

Although network services such as Telnet, FTP, and SNMP are used within the network interface boards, their use is necessary for the normal operating or service of these boards. Mechanisms have been implemented to restrict access to these services and, in addition, the implementation of client utilities for these services is further limited. These implementation considerations are in place to minimize the ability for a would-be perpetrator to use these boards a s a point to "hop-off" into the customers network or otherwise misuse these services.

The overall architecture represents a controlled and secure implementation of services and utilities necessary for ongoing maintenance and support of these boards. Precautions have been taken to minimize the use of these services and unnecessary utilities or services have been removed.

The combination of architecture, reduced services and clients, and restrictive mechanisms provide our customers with an overall offering that they may consider trusted and secure on their enterprise network.