Achilles Level 1 Certification Requirements for Network Devices: Gateways

Network Device Definition

A device which is required for the network to operate properly but does not interact directly with a control process. Network devices facilitate data flow between separate devices. Examples include routers, switches, gateways, and wireless access devices.

Test Setup

To test that the network device functionality is being correctly performed, a human-machine interface (HMI) is programmed to read and write data to an embedded device via the gateway, which is the device-under-test (DUT). For example, consider a scenario where the HMI writes to a PLC through a gateway and then reads the results: the HMI writes 1 to holding register A on the PLC; the HMI reads holding register A; the HMI writes 0 to holding register A; the HMI reads holding register A; repeat. The HMI measures the responsiveness of this process and associates this measured value with an OPC data tag. This tag is then made available to an OPC server so that it can be monitored by the Achilles OPC Monitor. Note that the HMI can measure the responsiveness of the register update process in two ways, depending on how the update is being conducted:

1. Open loop process: the register is written and read at constant intervals. For instance, at 0 msec, the HMI writes 1 to the register; at 500 msec, the register value is checked and if it is 1, the HMI writes 0 to the register; at 1000 msec, the register value is checked and if it is 0, the HMI writes 1 to the register; repeat. With this process, the vendor calculates the percentage of missed cycles for the past *n* seconds and stores this value in the OPC tag *missedCycles*. The value of *n* depends on how long it typically takes to update the register values.
2. Closed loop process: a new value is written to the register as soon as it changes. For instance, the HMI writes 1 to the register; the HMI then continually polls the PLC until the register value changes; the HMI writes 0 to the register; the HMI then continually polls the PLC until the register value changes; repeat. With this process, the HMI measures how long it takes for the register value to change from 0 to 1 and back to 0 and stores this value in the OPC tag *roundTrip*. Before testing begins, the average *roundTrip* value, *roundTripAVG*, is determined so that *roundTrip* values calculated during testing can be compared to a baseline value.

While the DUT is facilitating this operation, the Achilles™ Satellite executes the Achilles Level 1 Test Suite against it and monitors its behavior.

Pass/Fail Criteria

Test results are determined by the Achilles Satellite's OPC Monitor and ICMP Monitor. The status of each monitor must remain *Normal* during test execution, provided that the test case is executed on or below 10 percent link utilization. For example, on a 100 Mbit link, all test cases are executed at 10 Mbits/s or below. If a single test does not meet the aforementioned criteria, then the DUT fails Achilles Level 1 Certification.

Pass/Fail Criteria Exceptions

If the status of a monitor changes to *Warning* during test execution, an exception to the pass/fail criteria may be granted if the DUT's behavior is due to an explicit design decision. For example, suppose the DUT is designed to process up to 200 packets per second on a 100 Mbit link and ignore all traffic that exceeds this limit. Such behavior will likely result in the DUT not sending ICMP replies to the Achilles Satellite, resulting in an ICMP Monitor *Warning*.

To qualify for an exception, Wurldtech must accept that the exhibited behavior and the relevant design decision(s) are reasonable. The vendor must provide design documents that describe the device's behavior. Details of the exception to the pass/fail criteria will be made public, so the end user will be aware of the device's behavior. This practice is in line with Wurldtech's view that a key utility of certification is to ensure symmetric information between the customer and end user regarding a device's network robustness and resilience.

Key Parameters for Level 1 Certification

- Max link utilization: 10 percent.
- OPC Monitor: Timeout = For open loop processes *missedCycles* < 20%. For closed loop processes, *roundTrip* < *roundTripAVG* * 3.
- ICMP Monitor: Timeout = 0.5 seconds. Tolerable packet loss = 10 percent.

Test Cases and Parameters for Level 1 Certification

Test Case	Parameter Values
Ethernet Unicast Storm (L1)	Packet Length = 60, Rate Limit = 14880, Ethernet Protocol = IPV4, Duration = 120
Ethernet Multicast Storm (L1)	Packet Length = 60, Rate Limit = 14880, Ethernet Protocol = IPV4, Duration = 120, Multicast IP Address = Use multicast IPs from discovery
Ethernet Broadcast Storm (L1)	Packet Length = 60, Rate Limit = 14880, Ethernet Protocol = IPV4, Duration = 120
Ethernet Fuzzer (L1)	Number of Packets = 50000, Random Seed = Automatic, Source MAC Address = Local MAC, Destination MAC Address = Use DUT MAC
Ethernet Fuzzer (L1)	Number of Packets = 50000, Random Seed = Automatic, Source MAC Address = Local MAC, Destination MAC Address = Use multicast MACs from discovery
Ethernet Grammar (L1)	First Subtest = First in set, Last Subtest = Last in set

Test Case	Parameter Values
ARP Request Storm (L1)	Rate Limit =14880, Duration = 120
ARP Host Reply Storm (L1)	Rate Limit =14880, Duration = 120
ARP Cache Saturation Storm (L1)	Rate Limit =14880, Duration = 120, Random Seed = Automatic
ARP Grammar (L1)	First Subtest = First in set, Last Subtest = Last in set
IP Unicast Storm (L1)	Packet Length = 60, Rate Limit = 14880, Protocol = 17, Duration = 120
IP Multicast Storm (L1)	Packet Length = 60, Rate Limit = 14880, Protocol = 17, Duration = 120, Multicast IP Address = Use multicast IPs from discovery
IP Broadcast Storm (L1)	Packet Length = 60, Rate Limit = 14880, Protocol = 17, Duration = 120, Broadcast IP Address = Local Network
IP Fragmented Storm (L1)	Rate Limit = 812, Duration = 120
IP Fuzzer (L1)	First Packet = 1, Last Packet = 50000, Random Seed = Automatic, Bad IP Version = 50, Odd IP Header Length = 50, Fragmented Packets = 50, Source IP Address = Random, Destination IP Address = Use DUT IP
IP Grammar - Field Fuzzer (L1)	First Subtest = First in set, Last Subtest = Last in set
IP Grammar - Fragmentation (L1)	First Subtest = First in set, Last Subtest = Last in set
IP Grammar - Options Fields (L1)	First Subtest = First in set, Last Subtest = Last in set
ICMP Storm (L1)	Packet Length = 60, Rate Limit = 14880, Duration = 120
ICMP Grammar (L1)	First Subtest = First in set, Last Subtest = Last in set
ICMP Type/Code Cross Product (L1)	Packet Length = 60, Rate Limit = 14880, Protocol = 17, Duration = 120, Broadcast IP Address = Local Network
TCP Scan Robustness (L1)	Scan Mode =TCP SYN Scan, Destination TCP Ports = Use open ports from discovery, Use neighboring closed ports
TCP Scan Robustness (L1)	Scan Mode =TCP ACK Scan, Destination TCP Ports = Use open ports from discovery, Use neighboring closed ports
TCP Scan Robustness (L1)	Scan Mode =TCP FIN Scan, Destination TCP Ports = Use open ports from discovery, Use neighboring closed ports
TCP Scan Robustness (L1)	Scan Mode =TCP Connect Scan, Destination TCP Ports = Use open ports from discovery, Use neighboring closed ports
TCP Scan Robustness (L1)	Scan Mode =TCP Null Scan, Destination TCP Ports = Use open ports from discovery, Use neighboring closed ports
TCP Scan Robustness (L1)	Scan Mode =TCP XMAS Scan, Destination TCP Ports = Use open ports from discovery, Use neighboring closed ports
TCP SYN Storm (L1)	Rate Limit =14880, Duration = 120, Random Seed = Automatic, Destination TCP Ports = Use open ports from discovery, Use neighboring closed ports
TCP/IP LAND Attack (L1)	Rate Limit =14880, Duration = 120, Destination TCP Ports = Use open ports from discovery
TCP/IP LAND Attack (L1)	Rate Limit =14880, Duration = 120, Destination TCP Ports = Use open ports from discovery, Use neighboring closed ports
TCP Fuzzer (L1)	First Packet = 1, Last Packet = 50000, Random Seed = Automatic, Bad IP Version = 50, IP Options = 50, Fragmented Packets = 50, Bad TCP Checksum = 50, TCP Options = 50, Source TCP Port = Random, Source IP Address = Random, Destination TCP Port = First open port, Destination IP Address = Use DUT IP
TCP Grammar (L1)	Destination TCP Port = First open port, First Subtest = First in set, Last Subtest = Last in set
UDP Scan Robustness (L1)	Destination UDP Ports = Use open ports from discovery, Use neighboring closed ports
UDP Unicast Storm (L1)	Packet Length = 60, Rate Limit = 14880, Duration = 120
UDP Multicast Storm (L1)	Packet Length = 60, Rate Limit = 14880, Duration = 120, Multicast IP Address = Use multicast IPs from discovery, Destination UDP Ports = Use open ports from discovery, Use neighboring closed ports
UDP Broadcast Storm (L1)	Packet Length = 60, Rate Limit = 14880, Duration = 120, Broadcast IP Address = Local Network, Destination UDP Ports = Use open ports from discovery, Use neighboring closed ports
UDP Fuzzer (L1)	First Packet = 1, Last Packet = 50000, Random Seed = Automatic, Bad IP Version = 50, IP Options = 50, Fragmented Packets = 50, Bad UDP Checksum = 50, Source UDP Port = Random, Source IP Address = Random, Destination UDP Port = First open port, Destination IP Address = Use DUT IP
UDP Grammar (L1)	Destination UDP Port = First open port, First Subtest = First in set, Last Subtest = Last in set