Agilent N2X Packets and Protocols
Testing Access Control Lists

Application Note

Test your router’s access control lists with Agilent’s multi-port Packets and Protocols Application.

Access control lists (ACLs) serve as filters for controlling the traffic that enters or leaves a router’s interfaces. Primarily implemented for security reasons, ACLs instruct a router to block or forward traffic based on specific criteria, such as a packet’s source or destination address or an encapsulated upper-layer application, as indicated by the TCP port number.

ACLs are configured in firewall routers, border routers, or any intermediate router that needs to filter traffic. Separate lists are required for each network protocol the router supports, and each list contains multiple filter terms which must be tested to ensure that the router’s interfaces drop or forward all matching packets accordingly.

With Agilent’s N2X, you can quickly generate the right traffic to verify your router’s access control capabilities. This application note explains how to define streams that match specific ACL statements, then measure how well your device can apply these filter terms under realistic traffic loads.

Testing network devices has never been easier!

- Fine-grained measurements on up to 32k customers or services
- Quick and easy stream creation
- Powerful PDU builder designed for future flexibility
Testing with Agilent N2X

Agilent N2X is the industry’s most comprehensive test solution for testing the development and deployment of network services for converging network infrastructures. Service providers, network equipment manufacturers (NEMs) and component manufacturers can verify service attributes of entire networks end-to-end, while also isolating problems down to individual networking devices and subsystems.

Agilent N2X incorporates the strength of the RouterTester 900 to deliver unparalleled test realism to verify the ultimate performance, scalability and resilience of carrier grade services and infrastructure.

The N2X Packets and Protocols application enables N2X to verify the traffic forwarding performance, protocol scalability and services delivering capabilities of switching and routing devices across the enterprise, metro/edge and core.

A powerful and flexible PDU builder makes it easy to build streams of Layer-2 Layer-7 Protocol Data Units (PDUs) containing multiple encapsulations and even proprietary formats. With the PDU builder, you can define a packet length distribution and common header type, and then edit any field, including the payload. You can also set a field modifier to vary a header field’s values, creating a separate flow or measurable stream for each one. This tool reduces the time needed to generate multi-encapsulated traffic types thereby allowing you to get more out of your testing time.

Users can also generate and analyze more streams per port than any other tester available (up to 32,768 transmit and receive streams per port), making it easy to scale your tests beyond the maximum performance parameters of your network or device. Your test can include 256 test ports per system, with 15 traffic profiles and up to 1023 - 4095 stream groups per port, depending on the port type. In total, the Traffic Generation and Analysis application can generate and measure statistics on 32,768 streams per port, using either four separate measurements over 32,768 streams or twelve measurements over 4,096 streams.

Access control list (ACL) test

This application describes how to build traffic streams containing specific IP destination address and TCP destination port values, then measure the device’s ability to block or forward the streams according to the “deny” and “permit” statements in its access control lists.

Test configuration

As shown in the illustration below, a source test port sends streams that match ACL “permit” statements, streams that match ACL “deny” statements, and streams that do not match any of the statements to a destination test port through the device under test (DUT) to test its blocking and forwarding capabilities. Performance statistics are taken on the destination test port.

This test assumes your router’s interfaces are already configured with ACLs containing “permit” and “deny” statements that are based on IP destination addresses and TCP port numbers. However, you can easily adapt the test to fit other ACL filter criteria. For example, you can send Layer-2 traffic to match MAC source and destination address filter terms instead.
Test summary

Step 1: Select test modules and ports. Configure a source and destination test port on any N2X interface.

Step 2: Set up the physical and link layers. For extra information about these steps, click the Help button on the Physical and Link dialogs.

Step 3: Define the “deny” traffic. Use the new PDU builder to define a TCP/IP stream group containing IP destination addresses and TCP port values that match the “deny” statements in your ACLs. During this process, you can also create a separate, measurable stream for each destination address to verify that all traffic from the stream group is dropped.

Step 4: Define the “permit” traffic. Create a new set of “permit” streams to match the ACL “permit” statements with the PDU builder’s quick duplication feature.

Step 5: Define the general traffic. As in the previous step, quickly generate a third stream group that does not match any of the ACL statements. (Your router will either block or forward this general traffic, depending on its configuration.)

Step 6: Set the traffic properties. Define the traffic profile as constant or bursty, set the offered load, and specify the number of packets to send (e.g., continuous stream, n packets, or just one packet).

Step 7: Set up the statistics to view. Configure the destination test port to display a wide range of port- or stream-level performance measurements.

Step 8: Start traffic and measurements. View real-time packet loss measurements on the destination test port to verify that the DUT drops the correct traffic. You can also view the effect of filtering on the DUT’s general performance.

Step 9: Increase the offered load. Move N2X’s dynamic slider bar to increase the offered load while the test is in progress, then monitor the effect on the DUT’s performance.

Step 10: Stop the test. If you are sending traffic in Continuous mode, you must manually stop the test.

Step 11: Save the test configuration. You can save the entire test configuration as an XML file, including any profiles and streams you have defined.

---

Define, generate and analyze up to 32,768 traffic streams per port.

Easily scale the test bed by adding hundreds of additional ports.

Utilize Agilent’s unique PDU builder to ensure correct forwarding of standard, proprietary and experimental encapsulations.

Analyze latency, loss, throughput, QoS and other key performance attributes under varying conditions.
Generate a separate measurable stream for each IP destination address.

Create separate sets of streams with different IP destination addresses and TCP port values.

Edit the TCP destination port field value.
This page left intentionally blank.
This page left intentionally blank.
This page left intentionally blank.