Lumeta Data Glossary

This glossary endeavors to explain key Lumeta and network terminology embedded in API attribute names. For information on what is meant by *maximum degree*, *reference IP*, *SDS*, *stealth router*, *unauthorized perimeter router* and more, look no further.

Looking for a term that's not covered here? Let us know by submitting a request at the bottom of this page.

Alert

An Alert is an Lumeta event notification of finding a particular circumstance in the customer's network (during scanning and/or reporting) or regarding the Lumeta system itself. Alert generation is configured from the Admin tab of the Lumeta server, including whether the alerts are delivered to Syslog and/or IF-MAP.

Scanning and Reporting Alerts in Map's Node Details

System alerts and certain scanning and reporting alerts do not correspond to individual nodes on the Lumeta map.Scanning, Reporting, and System Alerts not in Map's Node Details

Alert Priority

A Priority of "Low" (0), "Med" (1), or "High" (2) is assigned to each alert, according to the alert configuration in effect when the alert is generated.

Alert Severity

A Severity of "Emerg" (0), "Alert" (1), "Crit" (2), "Err" (3), "Warning" (4), "Notice" (5), "Info" (6), or "Debug" (7) is assigned to each alert, according to the alert configuration in effect when the alert is generated. These possible values correspond to the traditional Syslog severities.

All Devices

Consolidated devices. A device is a piece of equipment that might respond on multiple IP addresses. All devices have at least one responsive IP.

Autonomous System (AS)

One of the ways Lumeta determines who owns the CIDR blocks. An autonomous system is a routing domain. By examining the autonomous system names contained in the Internet routers, Lumeta shows who makes routing announcements on the Internet for the specified devices or CIDR blocks.

Broadcaster

An IP address that, when pinged, produces multiple responses. Although these can be misconfigured IP addresses or misbehaving IP implementations, they are usually broadcast addresses. These can be analyzed to determine subnetting. Broadcasters eliciting a large number of responses may show networks that suffer from broadcast storms. As a general rule of thumb, a single packet sent to a broadcast address should not generate more than one or two thousand responses, at most.

Classless Inter-Domain Routing (CIDR) Block

A shorthand notation for a block of IP addresses, CIDR notation provides a more flexible and efficient way to define groups of IP addresses. Originally, the IP specification provided 4 types of IP address blocks, Class A through Class D addresses, which required the network prefix to be a multiple of 8 bits long. With CIDR notation, the network prefix can be any length from 1 to 32 bits, depending on the desired size of the network address block. Consequently, CIDR blocks are a much more efficient means to describe and route blocks of IP addresses. A typical CIDR block looks like: 198.152.185.0/24, where /24 indicates that the first 24 bits are the network prefix. This example represents a Class C network of 256 addresses.

Command Injection

Command injection is an attack method in which a hacker alters dynamically generated content on a web page by entering HTML code into an input mechanism such as a form field that lacks effective validation constraints. A malevolent hacker can exploit that vulnerability to gain unauthorized access to data or network resources. When users visit an affected Web page, their browsers interpret the code, which may cause malicious commands to execute in the users' computers and across their networks.

Community String

A router management password used by Simple Network Management Protocol (SNMP) v1 and v2c to allow queries to network devices.

Consolidated

A device may have more than one IP associated with it. We say that these IPs have been "consolidated" to a reference IP which is the IP used to, in most cases, refer to the device with which the IPs are associated.

DNS Labeling Format

DNS names appear, for instance, as one of the columns in the details page you open when you click on an IP address quantity within the report. The scanning machine looks up IP addresses using DNS PTR lookups for both internal and external domain name servers. A simple PTR response gives a name. If a domain name server returns a "non-existent domain" (NXDOMAIN), the report shows the name server that reported the error, in parentheses. A response that is listed as two parens () with nothing between them indicates a double-failure and should only happen on Internal DNS lookups. It indicates that not only did the DNS reverse lookup not return an associated name for an IP address, but also did not return a valid Start-Of-Authority (SOA) value. The absence of this value usually indicates a misconfigured DNS server. This should be very rare.

DNS Reverse Resolver
The domain name server delegated by the root servers to resolve reverse DNS requests for the specified CIDR blocks.

Domain Name Server
A domain name server translates domain names, such as www.lumeta.com, into IP addresses. Such servers are also called "name servers", while the service is called "domain name service" or "DNS".

Filtering Devices
Filtering devices are the unique IP addresses found which returned ICMP_UNREACH_FILTER_PROHIB (code 13), ICMP_UNREACH_HOST_PROHIB (code 10), or ICMP_UNREACH_NET_PROHIB (code 9). These codes are often returned by routers or firewalls that are blocking access. (Many devices return nothing and simply silently discard the packets.)

Hosts
Consolidated devices that were forwarding traffic and weren't determined to be switches based on SNMP.

Host Discovery
A detailed census of all IP addresses on the targeted networks.

IAB
Individual Address Block - The IAB is a particular OUI belonging to the IEEE Registration Authority, concatenated with 12 additional IEEE-provided bits, leaving only 12 bits of the MAC address for the vendor to assign to his (up to 4096) individual devices. An IAB is for companies who need less than 4097 unique 48-bit numbers and thus find it hard to justify buying their own OUI.

Inbound Leaking Devices
These external IP addresses are devices that were able to leak packet replies to internal IP addresses. An Lumeta Leak Discovery (LD) scan tests for leaks using two types of protocols: ICMP and UDP. ICMP-leaking devices were able to deliver a reply from an external Internet address to an internal IP address. UDP-leaking devices sent ICMP responses to UDP connection attempts to an internal IP address.

Inconclusive
A test of whether a port is active is classified as inconclusive if (a) filtering device(s) blocks access from all locations and reports the filtering activity to the scanning machine, (b) the device does not respond from any location (e.g., perhaps it is turned off in the middle of the test, an intermediate device filters the packets silently, packet loss), (c) the port appears to be active from some location(s), and inactive from other location(s), or (d) due to an unknown error.

IPv6 Enabled Router
A device accessible via an IPv4 network which responded to IPv6 SNMP OIDs.

Known List
The list of CIDR blocks that specifies the authorized and acknowledged extent of the network. Lumeta uses this list and the results of the network scan to generate the report. Any IP addresses discovered that are outside of this list are identified as "Unknown", and highlighted as anomalies for investigation. This list is defined when a report is initiated.

Leak Path Discovery (LD)
Lumeta's Leak Discovery (LD) scan determines if each host has connectivity to and/or from an external network (typically, the Internet) for ICMP and UDP, so that unauthorized connections are exposed. Types of unauthorized connectivity that Leak Discovery may uncover include telecommuters who are connected to the Internet via their personal Internet Service Provider (ISP) account while also connected to the corporate network via a virtual private network (VPN) and dual-homed systems within the network, such as web proxies.

Leaking Device
A leaking device is able to send and/or receive ICMP or UDP packets to or from the network containing the leak sensor (typically an external network, such as the Internet). An Lumeta Leak Discovery (LD) scan tests for leaks using two types of protocols: ICMP and UDP. ICMP-leaking devices were able to deliver a reply to an ICMP ping. UDP-leaking devices were able to send ICMP responses to UDP connection attempts.

Licensing Active IP Count
Unconsolidated IPs that responded during Host Discovery or Network Discovery as reported in all views.

Lumeta Network Index (LNI)
The Lumeta Network Index quantifies security risks in terms of the overall network, and the degree to which the defenses in the network expose end-devices to threats. Organizations can use the LNI to quantity the network risk factors associated with the current and changing state of their network over

time and to continually evaluate compliance with organizational security policies. The LNI provides the information needed to build a proactive network assurance program to minimize the risk profile of your network.

MAC Address
Media Access Control address -- a bit string that uniquely identifies an interface as the source or destination of transmitted frames at the data link layer. IEEE 802 MAC addresses are 48 bits long.

MAC Vendor
The company that registered with the IEEE for the right to manufacture network interface cards with certain assigned bits as the first portion of the MAC address. Lumeta determines the MAC vendor by comparing the first part of each MAC address discovered in the L2D scan with the IEEE-published lists of vendors who purchased specific OUIs and IABs.

Non-Responding Network
CIDR blocks scanned that did not respond from any sensor. A CIDR block may respond from some locations and may not respond from others. There are several possible reasons these networks were not seen during a network scan. Some reasons include (a) the CIDR blocks may not be in use in the network (b) they may be part of a firewalled network.

Organizationally-Unique Identifier
The first three octets of the MAC address. The OUI indicates the organization (typically a manufacturer) responsible for the unique assignment of the remaining 3 octets of the MAC address. OUIs are globally assigned by the IEEE.

Outbound Leaking Devices
These internal IP addresses are devices that were able to leak packet replies to the Internet. A Lumeta Leak Discovery (LD) scan tests for leaks using two types of protocols: ICMP and UDP. ICMP-leaking devices were able to deliver a reply from an internal IP address to an external Internet address. UDP-leaking devices sent ICMP responses to UDP connection attempts to an external IP address.

Perimeter
The network perimeter consists of the set of known routers that are the last known routers in any path from the known network to unknown space, or the first known routers in any path from unknown to known. These routers are termed Perimeter Routers.

Perimeter Router
A perimeter router is ordinarily the last router in the known network in a path between known space and unknown space, or the first known router in a path from unknown to known, but could alternatively be declared a perimeter router because of combining known and unknown IP addresses. (When Lumeta determines that a router has multiple interfaces, those IP addresses are consolidated into one router and one node on the map. If a router has at least one known IP address and one unknown IP address, it is declared a perimeter router -- even if it does not otherwise connect to unknown space, perhaps because it is an Unmapped Router.)

Point-in-Time Scan
A Lumeta scan of an enterprise network that is performed in a single sweep. Point-in-time scans are often scheduled to run on a repeat basis and serve to provide a historical record or audit trail for use by oversight agencies.

Private Address Space
Per RFC 1918, private address space is: 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16.

Real-Time Monitoring
Notification of network events-of-interest as they occur. Enables a system administrator to watch the current health, risk, processes, and vulnerabilities of a network through graphical charts and bars on a central interface/dashboard.Visual insights into the data are conveyed. Instant notifications/alerts into specific data-driven, administrator-specified events, such as when a data value goes out of range are provided.

Reference IP Address
When Lumeta determines that one device has multiple IP addresses, it represents that device with one "reference" IP address in the maps and in certain reports. From among the several IP addresses for a device, the reference IP address is chosen by this priority scheme:

- Address in Known CIDR covering the fewest IP addresses, rather than Unknown space.
- If necessary, address in Public realm, rather than Private (RFC-1918) realm.
- If necessary, address which is numerically lowest.

Router Degree
The router degree equals the number of other routers attached to that router. (A Sensor attached to that router is also counted.) The All Routers report lists the routers in descending order of connectivity, or degree. Routers with high degree may be good candidates for high-availability features or for redundant configurations. Unmapped Routers have zero degree.

Routing Devices
Consolidated devices that were shown to forward packets during Network Discovery.

Routing Loop
A routing loop is a path for which one or more probes passed through the same router twice. Some network designs produce routing loops when users attempt to access networks that aren't in use. Since the network doesn't exist, the loop goes unnoticed. The security concern is that unscrupulous users could use this knowledge to flood a link, thereby creating a Denial of Service (DoS) attack.

SNMP Details
This is a Tertiary Target type. If configured to do so, we will gather data from various SNMP OIDs and determine things like Interface or Route information

SNMP Accessible
A device that we were able to talk to and get responses with a set of SNMP credentials. If a device responds with sysDescr, interfaces, routes, the device is SNMP Accessible. If we just get an error message (an SNMPv3 credential error or a OID not found for v2) we will not be snmpAccessible though we will be an snmpResponder

SNMP Responder
A device that we got an SNMP response from even if we can't fetch data from it with our SNMP credentials. This could happen if we attempt to communicate with a device using SNMPv3, it can respond with an authentication error of some sort, this is different from SNMPv1/2c where the device usually doesn't send anything back in the case of an authentication failure (though ACLs can cause SNMPv2 errors).

SNMP v3 Alias
The Alias field of an SNMP v3 credential is an arbitrary label used to hide sensitive SNMP v3 credential fields in Lumeta reports. Acceptable field length is from 0 to 64 characters. If an Alias is not specified, an Alias will be generated from the hyphen-separated values of these SNMP v3 credential fields: Usern ame, Context Name,Authentication Protocol, and Privacy Protocol. The Alias is just for reporting purposes, and is not sent to the network during scanning, unlike all the other SNMP v3 credential fields.

SNMP v3 Authentication Password
The Authentication Password field of an SNMP v3 credential is used with the Authentication Protocol to complete the authentication of the SNMP v3 session. Acceptable field length is 8 to 64 characters (unless left empty because Authorization Protocol is None).

SNMP v3 Authentication Protocol
The Authentication Protocol field of an SNMP v3 credential is used to specify whether the protocol used for authentication of the SNMP v3 session will be MD5, SHA, or None.

SNMP v3 Credential
A credential is an associated set of fields used to allow queries to network devices via Simple Network Management Protocol (SNMP) v3. It is analogous to the Community String used in SNMP v1 and v2c.

SNMP v3 Context Name
The Context Name field of an SNMP v3 credential is the User-based Security Model (USM) field representing the context of the user's access. Acceptable field length is 0 to 32 characters. The empty context name (zero length) represents the default context.

SNMP v3 Privacy Password
The Privacy Password field of an SNMP v3 credential is used with the Privacy Protocol to complete the privacy (encrypting) of the SNMP v3 session. Acceptable field length is 8 to 64 characters (unless left empty because Privacy Protocol is None).

SNMP v3 Privacy Protocol
The Privacy Protocol field of an SNMP v3 credential is used to specify whether the protocol used for privacy (encrypting) of the SNMP v3 session will be AES, DES, or None. The use of privacy requires the use of authentication. That is, if the Authentication Protocol is None, then the Privacy Protocol must also be None.

SNMP v3 User Name
The User Name field of an SNMP v3 credential is the User-based Security Model (USM) field representing a user ID. Acceptable field length is 1 to 32 characters.

Stealth Routers
Stealth routers are hops on a path that did not respond to packets Lumeta sent to discover paths during ND and during the phase of HD that discovers paths to every IP address. Lumeta scans outward from a sensor, one hop at a time, toward each target network by sending a series of packets with increasing time-to-live (TTL) values. Most routers respond properly to packets with TTL values of zero by sending a TTL-exceeded notification back to the sender. However, some routers (especially Linux systems) limit the number of ICMP responses per second, while others simply do not respond properly. If the user has configured the scan to allow some number of stealth hops, Lumeta initially skips over the non-responding router and tries the next hop. If it responds, Lumeta continues and returns to try the non-responding routers again later. If a certain (user-configurable) number of hops in a row do not respond, Lumeta assumes the scan has hit a firewall or black hole and stops pursuing that path. If Lumeta never gets a response from that router, it records a "Stealth Router."

Target List
The list of CIDR blocks that specifies the network to be scanned. Any IP addresses discovered that are outside of this list are identified as "Untargeted", and highlighted as anomalies for investigation. This list is defined when a scan is initiated.

Total Active IPs
Unconsolidated IPs associated with a responsive device. These may include interface IPs even if the IP wasn't responsive.

Total IPs
All unconsolidated IPs. This includes IP addresses found in MAC tables on devices.