Practical Network Defense notes

Matteo Salvino

Contents

1 Network 101

Internet is in essence a network of networks with a hierarchical structure. The path into the Internet backbone could be wired or wireless. The backbone itself consists of global Internet Service Providers (ISPs) and several regional ISPs that are all interconnected to provide a path from sender to receiver. The communication path may typically contain a variety of switches and routers that facilitate and direct the flow of information through the network. The communication links, regardless of whether they are wired or wireless, are defined by a transmission rate and bandwidth. Access networks are used to connect a host or Local Area Network (LAN) to the Internet. Routers connect LANs, generate routing tables and forward packets of data on their path from source to destination. The Internet backbone, also called network core, is basically a group of routers interconnected by optical fiber as well as DNS servers containing infrastructure name servers, such as root Domain Name Servers (DNSs) employed for naming. The remaining components in the Internet structure that lie outside the network core, are simply access networks. An individual home network can be considered a small network or subnet. The Internet uses a gateway, also known as an edge router, to connect these networks to the edge of the network, also called network edge. The network core is composed of a set of routers and fiber links. The routers work together to determine the most efficient routing path for a packet from source to destination. A distributed algorithm is used that provides the flexibility to adapt to changing conditions, and routing tables are generated and maintained in real time. The core is provided by ISPs that interconnect multiple continents, called Global ISPs or Tier-1 ISPs, whereas the Regional ISPs are known as Tier-2 ISPs. The tier-1 ISPs that form the Internet backbone are interconnected at various access points called **Internet eXchange Points (IXPs)**. It would certainly appear that the intercommunication among computers would require some standardization that would facilitate their successful interactions. There should be some "protocol" that defines the manner in which they talk to each other so that messages are clearly understood. It is this "protocol", documented in a stack that is accomplished through modularization, development and upgrades that support operations such as web surfing, email, etc. By its very structure it is clear that the stack consists of different layers, each of which performs a special function. Modularization of the Internet is accomplished through layering. As a result, the Internet is being developed by many people, and institutions through a divide-and-conquer strategy. There is a strong interaction between layers in that each layer relies on the

services of the layer below and exports services to the layer above. It's the interface between layers that defines the interaction, for example implementation details can be hidden and layers can change without affecting other layers. Access layer is constituted by network with the same end-point, and the protocol used is Ethernet. Each host in a Ethernet network has a Network Interface Card (NIC) with a fixed address. MAC addresses uniquely identify hosts in the network and each of them processes packets intended for it. An ethernet network constitutes a broadcast domain, where each ethernet frame is received by all hosts. Actually, switches segment the network to limit the explosion of packets in the network, and only broadcast message are replicated. Switches remembers the source MAC addresses on the different ports. They only replicate the frame on the segment where the destination MAC address replies, with the support of ARP tables (for hosts) and CAM tables (for switches). Ethernet cannot be used for the entire Internet because of its broadcast packets, that would be highly inefficient for large networks. There is the need of a logical division of the networks : while Ethernet provides the Access layer, the Distribution layer is based on **Internet Protocol (IP)**, which is at level of Autonomous Systems (like big enterprises and ISPs). The main difference between Ethernet and IP address is that the first one is a physical addresses, so we cannot change the MAC address of our NICs, and tell who you are but not where you are, the second one is a logical address, so we can change the IP address of our NIC and is used to identify and reach networks and hosts. If two hosts belongs to the same network, then they can communicate using local addresses, otherwise they must use remote addresses. In order to know if one IP is in the same network than you, we can use the subnet mask. There are two version of IP addresses :

- **IPv4** : it defines IP address with 32 bits organized in four octects (8 bits in each)
- **IPv6** : has 128 bits.

For human readability the bits in each octet are separated by dots while writing an IPv4 address and colons in IPv6. IP addresses, regardless its version, are constituted by a network part and an host part, where the subnet mask defines precisely the boundary between them. There are three types of IP addresses :

- **Unicast** : these refer to a single destination host
- **Broadcast** : these refer to every host on a network or subnet

- **Multicast** : these refer to a group of IP addresses in a network, not necessarily all of them.

IP addresses has been classified in the following classes :

- Class A (24 bits for host addresses)
- Class B (16 bits for host addresses)
- Class C (8 bits for host addresses)
- Class D (multicast)
- Class E (reserved).

There are routable and non-routable address ranges. The first one need to be unique on the Internet (public), while the second ones (private, e.g. from 10.0.0.0 to 10.255.255.255, from 172.16.0.0 to 172.31.255.255, from 192.168.0.0 to 192.168.255.255) are defined in RFC 1918. Since each set of 8-bits can hold values from 0-255 we haven't flexibility at all. The idea is to use a Variable Length Subnet Mask in order to use a specific length of the subnet mask based on our needs. Many smaller networks can be grouped using the supernetting technique. In point-to-point links the subnet 31 is allowed. Other ways to reduce the waste of IP addresses in a subnet are NAT and IPv6.

2 Traffic monitoring

It's important to note that activities within the Internet can be approached in a modular fashion and this modularization is accomplished through layering. It is clear that the stack consists of different layers, each of which performs a special function. There is a strong interaction between layers in that each layer relies on the services of the layer below and exports services to the layer above. The task of a layer involves the exchange of messages that follow a set of rules defined by a protocol. When computers are connected with a network, guidelines must be established that support their interaction. The architecture that defines the network functionality is split into layers that collectively form what is commonly known as a protocol stack. Lets talk about **OSI model**. Each layer of the protocol stack may employ several protocols t implement the functionality of that particular layer. In a natural progression up the stack, the physical layer deals with the transmission of bits that are propagating over such media as copper, fiber or radio.

The data link layer aggregates the bits (e.g. in a frame), and performs the data transfer between neighboring network elements using as an example, Ethernet or WiFi. The network layer handles the routing of datagrams, in packet form, from source to destination using routing protocols. The transport layer performs the process-to-process communication using segments, i.e. message transfer using for example TCP. The session layer aggregates connections for efficiency, synchronization and recovery in data exchange. The presentation layer permits applications to deal with coding, encryption, and so on. Finally, we have the application layer which allow the user to invoke protocols for information exchange. Another well known model is **TCP/IP**. It's constituted by four layers : application layer corresponds to the top three layers of the OSI model, transport layer is equivalent to the transport layer of the OSI model, Internet layer is equivalent to the network layer of the OSI model, Datalink is equivalent to the data link layer of the OSI model and physical layer is equivalent to the physical layer of the OSI model. The layer ideal representation is that transport represent the illusion of direct end-to-end connection between processes in arbitrary systems, network transfers data between arbitrary nodes and data link transfers data between directly connected systems (via shared medium or direct cable). Each layer in the stack, with the exception of the physical layer, has a **header**. These headers facilitate the communication of information and are analogous to an envelope that contains both source and destination addresses. The link layer has a header containing MAC addresses, the network layer has a header containing IP addresses and the transport layer has a header containing the port number (i.e. service number). The port range is [0..65535], where the source port is randomly chosen by the OS and the destination port determines the required service. The port range [0 ..1023] contains well-known ports and they are used by servers for standard internet applications (e.g. 25 for SMTP, 80 for HTTP, 143 for IMAP). The ports in the range [1024..49151] can be registered with Internet Application Naming Authority (IANA), whereas ports in the range [49152..65535] are called ephemeral ports. Protocols are classified in two main categories :

- **connection oriented** (like TCP) : these protocols perform a number of very important functions. For example, they govern the movement of packets from source to destination under the specifications of certain standards, take actions that are specified in the packets, manage packet flow and congestion for optimal performance and even recover lost packets. The protocols work in conjunction with one another to accomplish the specified task required by the user.

- **connectionless** (like UDP) : these protocols doesn't provide any guarantee that the datagram is really deliver to the correct destination (i.e. there isn't control on data exchange). Furthermore, there isn't a possibility to recover from errors and manage the flow congestion.

The procedure to open a TCP connection between two hosts, A and B, is called three-way handshake, which is constituted by the following steps :

1. A sends a SYN segment to B with the sequence number field that contains the value x, which specifies the initial sequence number of A.

2. B sends a SYN and ACK segment to A, where the sequence number field contains the value y, which specifies the initial sequence number of B and the ack field contains the received value x increased by one.

3. A sends an ACK segment to B, where the sequence number field contains the value x + 1 and the ack field contains the received value y increased by one.

Packets that flow in the network can be captured using a network traffic dump tool, like dumpcap, wireshark or tcpdump. All of them can visualize and store the captured data, while the last two can also analyze the captured packets. In wireshark data from a network interface are "dissected" in frames, segments and packets, understanding where they begin and end. Then, they are interpreted and visualized in the context of the recognized protocol. When we captures packets, we collect a lot of them, so to make our life easier we can use filters. In fact, they allows us to only focus on requested packets or certain activity by network devices. Filters are divided in : display filters in order to inspect only the packets we want to analyze once the data has been processed, and capture filters in order to limit the amount of network data that goes into processing and is getting saved. In the second one the packets not captured are lost, where in display filters we display only captured packets matching the filter, without discard them. Frames are collected from the interface and passed to several, consecutive, "dissectors" one for each layer (they are passed from the bottom layer to the upper one). Protocols can be detected in two ways :

- **Directly** : if a frame has the field that explicitly states which protocol it is encapsulating.

- **Indirectly** : with tables of protocol/port combinations and heuristics.

We can capture network traffic in different modes :

- **promiscuous mode** : cannot fetch every packet due to network segmentation.
- **physical tap** : device that mirrors traffic passing between two network nodes.
- **port mirroring** : a port of the switch which mirror all the traffic.
- **aggressive approaches** like :
  - **ARP poisoning** : send ARP replies to steal IP addresses
  - **MAC flooding** : fill the CAM table to make switch act like an hub.
  - **DHCP redirection** : exhausts IP addresses of the pool and then pretends to be the default gateway of the network with the new DHCP requests.
  - **ICMP redirection** : use ICMP type 5 message to indicate a better route.

Now, the question is How to prevent packet capture ? We can use two different approaches :

- **Dynamic address inspection** : validates ARP packets with IP-to-MAC inspection by intercepting every ARP request and dropping the invalid ones (placed on switches).
- **DHCP snooping** : always implemented in switches, it distinguishes between trusted and untrusted ports and uses a database of IP-to-MAC. Ports that show rogue activity can also be automatically placed in a disabled state.

3 IPv6 introduction

IPv4 provides for a maximum 4.29 billion 32-bit addresses, which seemed like more than enough addresses when IPv4 became a standard in 1980. The number of IP addresses needed today far exceeds the world's population for several reasons. First of all, IPv4 addresses are often allocated in groups of addresses, as network addresses. Places such as companies, schools and airports are allocated network addresses for their users. But a much larger reason we need so many more IP addresses is the number of devices per

person that are being connected to the Internet. IPv6 provides more addresses than IPv4. In comparison, the 128 bit IPv6 address space provides for 340 undecillion addresses (i.e. approximately 2^128). The number of people accessing the Internet is increasing dramatically. Even with short-term solutions like NAT, we are in the final stages of public IPv4 address availability. There has also been extraordinary growth in the number of devices connected to the Internet. IANA assigns IPv4 addresses to the five Regional Internet Registries (RIRs) in /8 address blocks. Using this address space, RIRs then ridistribute the IPv4 network addresses to ISPs and other end customers. On January 31, 2011, IANA allocated the last two blocks of IPv4 address space to RIRs. At this point, IANA had now run out of IPv4 addresses. This doesn't mean that IPv4 addresses are no longer available for end customers, but they can still get them from most ISPs. However, many ISPs are severely limited. So, in the early 1990s, IETF began the development of a new version of IP known as **IP Next Generation**, which later became **IPv6**. However, IPv6 was a long-term solution, and a short-term solution was needed immediately. Several short-term solutions were put into place. Two of the most important were **CIDR** and **NAT** with private IPv4 addresses. We know how CIDR allocates IP addresses. NAT along with private IPv4 addresses has been the reason IPv4 has survived all these years. It allows multiple hosts using private IPv4 addresses within their internal network to share one or more public IPv4 addresses when accessing the global Internet. NAT has also some critical points. At the very least, NAT means that our routers, application gateway and other devices must perform extra processing to make NAT work, which also causes latency. Other points are that it breaks peer-to-peer networking and accessing our "hidden" system from other networks. The IETF never intended NAT to be used for security. We want to say that in the late 1970s, a family of experimental protocols, known as **Internet Stream Protocol (ST)**, and later **ST2**, was developed. ST was an experimental resource reservation protocol intended to provide Quality of Service (QoS) for real-time multimedia applications such as video and voice. Although it was never recognized as **IPv5**, when encapsulated in IPv4, ST uses IP version 5.

3.1 Notation and types

IPv6 is much more than just a larger source and destination IP address. Developers of IPv6 took this opportunity to not only improve IP but also many of the protocols and processes related to IP. In fact, the benefits on IPv6 include : larger address space, stateless autoconfiguration, end-to-end

reachability without private addresses and NAT, better mobility support, peer-to-peer networking easier to create and maintain, and services like VoIP and QoS become more robust. An IPv6 address is 128 bits in length and hexadecimal is the ideal number system for representing long strings of bits. Every 4 bits can be represented by a single hexadecimal digit, for a total of 32 hexadecimal values from 0000 to FFFF. AS described in RFC 4291, the preferred form to represent an IPv6 address is x:x:x:x:x:x:x:x. Each x is a 16-bit section that can be represented using up to four hexadecimal digits, with the sections (also called **hextets**) separated by colons. The result is eight 16-bit sections for a total of 128 bits in the address. There exists some rules in order to reduce the notation involved in the preferred format such as :

1. **omit leading 0s** : one way to shorten IPv6 addresses is to omit leading 0s in any hextet. This rule applies only to leading 0s and not to trailing 0s (because omitting both would cause the address to be ambiguous).

2. **omit all 0s hextets** : the second rule for shortening IPv6 addresses is that you can use a double colon (::) to represnet any single, continuous string of two or more hextets consisting of all 0s. If there are multiple possible reductions, RFC 5952 states that the longest string of zeroes must be replace with double colon and if they are equal then only the first string of 0s should use the :: representation.

An IPv6 address can be **unicast**, **multicast** and **anycast**. A unicast address uniquely identifies an interface on an IPv6 device. A packet sent to a unicast address is received by the interface that is assigned to that address. Similar to IPv4, a source IPv6 addresses must be a unicast address. In the following sections we will deeply describe the previous types of IPv6 addresses.

3.1.1 Unicast address

An unicast IPv6 address in turn can be :

- **Global Unicast Address** : it's a globally routable and reachable address in the IPv6 Internet. They are equivalent to public IPv4 addresses. Its generic structure has three fields :

  - **Global Routing Prefix** : it's the prefix or network portion of the address assigned by the provider to the customer site.

- **Subnet ID** : the subnet id is a separate field for allocating subnets with the customer site. Unlike with IPv4, it's not necessary to borrow bits from the Interface id (host portion) to create subnets. The number of bits in the subnet id falls between where the GRP ends and where the interface id begins.
- **Interface ID** : it identifies the interface on the subnet, equivalent to the host portion of anIPv4 address. The interface id in most cases is 64 bits.

Except under very specific circumstances, all end users will have a global unicast address (or more than one). It's range is from 2000::/64 to 3fff:fff:fff:fff::/64.

- **Link-Local Unicast Address** : a link-local address is an unicast address that is confined to a single link, a single subnet. They needs to be unique on the link and don't needs to be unique beyond the link. Therefore, routers do not forward packets with a link-local address. Link-Local Unicast addresses are in the range of fe80::/10 to febf::/10. The following 54 bits are recommended to be all 0s and 64 bits dedicated to the Interface id. They are created in two ways :
  - **Automatically** : an IPv6-enabled device must have a link-local address. By default, devices automatically create their own link-local unicast addresses. The prefix is typically fe80::/64, followed by a 64 bit interface id that is automatically generated in one of the two ways :
    - **EUI-64** generated : the IEEE defined the EUI process using the interface's Ethernet MAC address to generate a 64-bit interface id. When EUI-64 is used to create a link-local address, the fe80::/64 prefix is prepended to EUI-64 generate interface id. An Ethernet MAC address is 48 bits, a combination of a 24 bit Organizationally Unique identifier (OUI) and a 24 bit Device Identifier, written in hexadecimal. The EUI process is an insertion of 16-bit value of fffe between the 24 bit OUI and the 24 bit device identifier, with the Universal/Local bit flipped (7th bit of the first byte).
    - **Randomly generated** : EUI-64 is a convenient technique for automatically creating a 64 bit interface id from a 48 bit MAC address. However, it introduces a concern for some users : the ability to trace an IPv6 address to the actual

physical device using the 48 bit MAC address. To alleviate this privacy concern, devices can use randomly generated 64 bit interface ids.

- **Static** : the disadvantage of an automatically generated link-local address is that the long interface ID is difficult to recognize. It's much easier to use a simpler, manually configured ink-local address that is easier to identify.

3.2 Addressing

Using **ICMPv6 Neighbor Discovery Protocol** Router Solicitation and Router Advertisement messages, hosts determine how to obtain their IPv6 addressing information dynamically. If SLAAC is used, the host can automatically obtain IPv6 addressing information, such as prefix, prefix length, and a default gateway address. The default gateway address is a link-local address, the IPv6 source address of the Router Advertisement message. ICMPv6 ND includes similar processes as in IPv4, such as address resolution, router discovery, and redirect, but also with some significant differences like prefix discovery, Duplicate Address Detection (DAD) and Neighbor Unreachability Detection (NUD). Neighbor Discovery uses five ICMPv6 messages :

- **Router Solicitation** message |
- **Router Advertisement** message | for router-device messages used with dynamic address allocation
- **Neighbor Solicitation** message |
- **Neighbor Advertisement** message | for device-device messages used for address resolution
- **Redirect** message | for router-device messages used for better first-hop selection.

A host sends a Router Solicitation message when it needs to know how to dynamically obtain its addressing information. This typically occurs during startup and is the default on most host operating systems. A Cisco router sends Router Advertisement messages every 200 seconds by default, and it also sends an RA message upon receiving a Router Solicitation message from a device. The RA message is a suggestion to devices on the link about how to obtain their addressing information dynamically. The RA message is sent to all IPv6 devices multicast address. The RA message contains three flag :

- **Address Autoconfiguration** flag (A flag) : when set to 1, which is the default setting, this flag tells the receiving host how to use SLAAC to create its global unicast address. SLAAC allows the host to create its own GUA address by combining the prefix in the RA message with a self-generated interface id (using EUI or randomly generated).

- **SLAAC with Stateless DHCPv6** flag (O flag) : when set to 1 (default setting is 0), this flag tells the host to obtain other addressing information, other than its GUA, from a stateless DHCPv6 server. This information may include DNS server addresses and a domain name.

- **Managed Address Configuration** flag (M flag) : when set to 1 (default setting is 0), this flag tells a host how to use a stateful DHCPv6 server for its GUA and all other addressing information. This is similar to DHCP for IPv4. The only information the host uses from the RA message is from the RA's source IPv6 address, which it uses as the default gateway address.

In the second case after a device generates one or more addresses using SLAAC, it contact a stateless DHCPv6 server for additional information. Remember that a stateless DHCPv6 server doesn't allocate or maintain any IPv6 global unicast addressing information. A stateless server only provides common network information that is available to all devices on the network, such as a list of DNS server addresses or a domain name. In particular, a host after obtained its own GUA sends out a DHCPv6 SOLICIT message to all DHCPv6 servers multicast address. One or more DHCPv6 server respond with a DHCPv6 ADVERTISE message, indicating that they are available for DHCPv6 service. The host responds to the selected server by sending an information REQUEST message, asking for other configuration information. The selected DHCPv6 server responds with a REPLY message that contains the other configuration information.

In the third case, stateful DHCPv6 doesn't utilize SLAAC to generate a GUA. A stateful DHCPv6 server provides IPv6 GUAs to clients and keeps track of which devices have been allocated which IPv6 addresses. A significant difference between stateful DHCPv6 and DHCPv4 is the advertising of the default gateway address. In IPv4, the DHCPv4 server usually provides the default gateway. In IPv6, only the router transmitting the ICMPv6 Router Advertisement can provide the address of the default gateway dynamically. There is no option within DHCPv6 to provide a default gateway

address. A host after receiving the RA uses the source IPv6 address of the RA as its default gateway address. Then addressing and other configuration information is available from a stateful DHCPv6 server. So, the host sends out a DHCPv6 SOLICIT message to all DHCPv6 servers multicast address, searching for a DHCPv6 service. One or more DHCPv6 server respond with a DHCPv6 ADVERTISE message, indicating that they are available for DHCPv6 service. The host select one DHCPv6 server by sending to it a DHCPV6 REQUEST message asking for addressing and other configuration information. The selected DHCPv6 server responds with a reply message that contains a GUA and other configuration information. Finally, the host perform DAD on the address received from the stateful DHCPv6 server to ensure that this address in unique.

To ensure unicast address uniqueness, address resolution procedure includes **Duplicate Address Detection (DAD)**. The device sends a Neighbor Solicitation message for its own IPv6 address to detect whether another device on the link is using the same address. If a Neighbor Advertisement message is not received, the device knows its address is unique on the link.

3.2.1 Prefix Delegation process

In the world of IPv4, most internal networks use a private IPv4 address space for internal devices and NAT at the edge router to translate an address to a globally routable public IPv4 address. This is a common mechanism for most home networks and is partly responsible for keeping IPv4 alive for so many years. Avoiding the complications and problems with address translation, IPv6 uses a different technique. One of the methods IPv6 uses is DHCPv6 with the **Prefix Delegation** option, which provides a mechanism for automated delegation of globally routable IPv6 prefix from a provider's router to a customer's router using DHCPv6. In this process are involved two routers :

- **Requesting Router (RR)** : this is the router that acts as the DHCPv6 client, requesting the prefix(es) to be assigned.
- **Delegating Router (DR)** : this is the router that acts as the DHCPv6 server, responding to the requesting router's IPV6 prefix request.

Lets describe in details the Prefix Delegation process. First the RR's ISP facing interface needs an IPv6 address, that can be dynamically obtained using SLAAC, stateless or stateful DHCPv6 server. Then the RR initiates

DHCPv6-PD in its SOLICIT message by including a request for an IPv6 prefix. The REPLY message from the DR (the ISP router) includes the IPv6 prefix. This is the prefix that the RR can use for its own internal network (i.e. a prefix that the RR can use to allocate addresses to its client).