DEPARTMENT OF COMPUTER AND SOFTWARE ENGINEERING

Muawiz Umer CE-42-A

CN-Assignment 03

TASK :

Network address translation (NAT) helps multiple hosts to connect to the Internet using a single public IP address. NAT traversal is a CN technique which establishes and maintains IP connections across gateways that uses NAT.

- Hole punching is a technique where the source and destination IP addresses of a packet are replaced by an intermediate node prior to transmission. It is used in applications such as voice over IP (VoIP), instant messaging, and email. Hole punching is an alternative to using relaying schemes.
- It is also important to note that hole punching is not intended to replace traditional network address translation (NAT). Rather it should be used in conjunction with NAT when one or more endpoints are behind firewalls that prevent their public IP addresses from being visible outside the network.

TCP/UDP hole punching schemes with scenario-based examples.

- The hole punched TCP/UDP hole punching scheme is an extension of the TCP/IP packets to allow the data to be sent to a different destination than that of the original sender. The sending host sends a special UDP or TCP packet to an application layer gateway (ALG) that interprets that packet and inserts it in a new TCP segment for transmission out of the sending host.

This section describes how this works, including the following topics:

How does a TCP/UDP hole punch work? What are some scenarios?

Why might you want to use it?

- In a TCP/UDP hole punching scheme, the hole punch is a special sequence number that is used to indicate that an IP packet can be duplicated. This allows the IP layer to send a duplicate message with a modified header. The receiver uses this information to reconstruct the original message correctly.

The following example uses UDP to show how hole punching works:

The host sends a packet with a destination port of 10001 and source port of 10002.

The host sends another packet with the same IP address but with a different source port number 10003.

The host receives both packets and combines them into one large packet so it can send it out on port 10001.

Hole punching is a mechanism for inserting an acknowledgment message into the TCP/IP stream that requests a retransmission. The acknowledgment message carries the same sequence number as the last packet received. If the next packet arrives with a new sequence number, then it can be forwarded to the destination without disturbing any other TCP connections.

Hole punching can be used either at the end of data transmission or in-band on top of existing data (e.g., during a retransmission). The hole punching mechanism is also referred to as hole punching scheme, hole punch, or "hole" retransmission. Hole punching uses two separate streams: one for data and one for acknowledgments (ACKs). For example, if a TCP connection has three segments in flight and you receive an ACK for segment 2, you send another ACK so that the data stream resumes without missing any packets.

Hole punching is an optimization problem in which the objective is to maximize or minimize a function of the number of packets dropped by a router.

In TCP/UDP hole punching, the objective is to minimize the number of packets dropped at the ingress router and at the egress router. Hole punching can be thought of as a form of resource allocation problem where resources are holes in a transmission channel. The goal is to find an optimal hole-punching strategy that maximizes throughput while minimizing loss.

The classic hole punching algorithm for TCP/UDP uses two pseudo-randomly selected routers to achieve an uneven load on each router. The first switch (S1) sends data to Router A and Router B alternately, with each switch sending twice per round trip time interval. A similar scheme is used except that S2 sends data only to Router A and Router B alternately, with each switch sending once per round trip time interval. This scheme has been shown to work well for very high bandwidth links such as those found on satellite links or fiber links with long distances between switches.

Analysis:

An important part of the TCP/UDP hole punching scheme is the use of a relay. The relay is a device that can forward packets between two hosts in the absence of a direct link between them. It therefore acts as an intermediate router, and its role is to connect two networks that are not directly connected.

The problem with the relay approach is that it requires the use of more than one device, which increases complexity and cost. It also introduces some delay as an additional step in the process. This is why some researchers have tried to find ways to reduce this complexity and cost by using algorithms other than relays.

Hole punching is a new scheme for hole punching that is more complex than the relay scheme, but does not require as many relays. The idea behind this scheme is to use multiple paths between two points in order to increase the reliability of the connection. This can be done by having multiple nodes on each side of a connection and having each node route data through the least loaded path. This allows multiple connections to be made with less overhead than using a relay scheme would have. However, this approach has its own set of problems. For example, if one of these connections fails at any point in its life cycle, then all other connections will fail as well unless they are also using this scheme. The hole punching scheme is a recommended approach to mitigate the TCP/UDP hole punching attack. This mechanism uses a relay agent to send packets to the destination address with the hole punch packet, which can be used as an addition when the original packet is not in the state of being blocked.

The core idea of this proposed scheme is that the relay agent sends a new packet with a hole punch value to the destination address after receiving an original packet with a hole punch value from the source address. The original and new packets are not sent by different hosts, but they are sent by different relays. This approach has two advantages:

(1) It does not require any modifications to application software at all;

(2) It does not require any modification in routers or switches, because all packets are received through regular interfaces and forwarded to their destinations.

THE END