

A white paper with black text and numbers

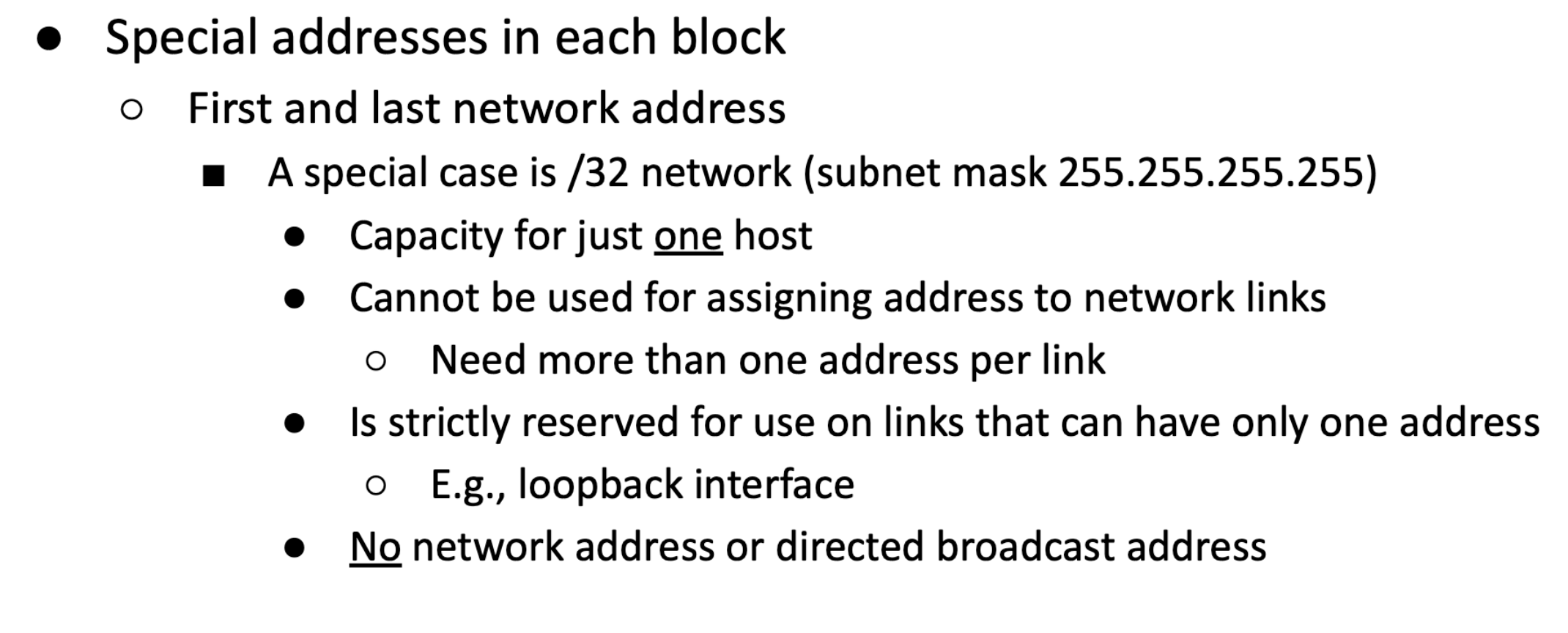
Description automatically generated

A white and black document with numbers and black text

Description automatically generated

A close-up of a computer screen

Description automatically generated



A white paper with red text and black text

Description automatically generated

**NAT**

 **NAT** allows internal networks to use private IP addresses and share a single or a pool of global IP addresses for communication with the Internet.

 **Address translation** is done by the NAT router, which replaces the private IP with a global IP for outgoing traffic and vice versa for incoming traffic.

 **PAT** (Port Address Translation) allows multiple internal hosts to share the same global IP by using unique port numbers for each connection, solving the problem of limited global IP addresses.

 NAT works well for client-initiated traffic but may have limitations for server-initiated communications.

BITTORRENT:

 **HTTP’s Problem**: Normally, when you download a file via HTTP (like clicking a link), the server has to upload the file to every person who wants to download it. This can be expensive for the server, especially if many people are downloading the file at the same time.

 **BitTorrent’s Solution**: BitTorrent solves this by having people who are downloading the file also upload pieces of it to each other. This way, the cost of uploading is shared among all the downloaders.

**The .torrent File**: When someone wants to share a file, they create a **.torrent file** and upload it to a web server. This small file contains information about the file being shared

**The Tracker**: The **tracker** is a server that helps people find each other. When someone starts downloading the file, the tracker tells them which other people (called **peers**) are also downloading it. Downloaders connect to each other directly.

Each peer downloads pieces of the file and uploads those pieces to other peers.

**Pipelining:** BitTorrent uses pipelining to keep the download fast. Instead of waiting for one piece to finish downloading before requesting the next, it requests several pieces at the same time, ensuring that there’s always data being downloaded.

**PIECE SELECTION:**

** Strict Priority:** Once a peer starts downloading a piece of the file, it finishes that piece before moving on to another. This helps make the download process smoother.

** Rarest First**: Peers download pieces that are the rarest first (meaning pieces that fewer peers have). This ensures that these rare pieces get shared quickly so no part of the file becomes unavailable.

** Random First Piece**: At the start, peers download random pieces to quickly get a complete piece. This allows them to start uploading to others as soon as possible.

** Endgame Mode**: Near the end of the download, BitTorrent requests any remaining pieces from all available peers to make sure the download finishes quickly.

**TERMS:**

** Choking: This is when a peer temporarily stops uploading to another peer. It doesn’t stop downloading, though, and the connection remains open.**

** Pareto Efficiency: This economic concept means that no two peers can improve their situation without making someone else worse off. BitTorrent tries to reach this balance by using tit-for-tat to ensure fairness.**

** Tit-for-Tat: Peers upload to those who upload to them, ensuring that people share fairly. If a peer isn’t uploading, they might get choked, meaning others won’t upload to them.**

**CHOKING ALGOS**

**4.1 BitTorrent’s Choking Algorithm**

* **Choosing Peers to Upload To: Each BitTorrent peer unchokes (uploads to) a certain number of peers at a time. Peers decide who to unchoke based on their current download rate. Every 10 seconds, peers recalculate who they want to upload to.**

**4.2 Optimistic Unchoking**

* **Finding New Connections: BitTorrent always unchokes one peer at random, even if that peer isn’t currently providing good download rates. This helps discover new peers that might have better bandwidth. Every 30 seconds, BitTorrent tries a new peer as its optimistic unchoke.**

**4.3 Anti-snubbing**

* **Handling Poor Download Rates: If a peer hasn’t received any pieces from others in a while, BitTorrent assumes it’s being “snubbed” and prioritizes finding new peers to download from.**

**4.4 Upload Only**

* **When Done Downloading: Once a peer has finished downloading the file, it no longer needs to decide who to upload to based on download rates. It switches to preferring peers that it can upload to quickly.**

**ICN Paper:**

** ICN: A new model that focuses on retrieving data by its name rather than the location of the data (IP address). users request content by name, and the network finds and delivers the content from the nearest source.**

** Coexistence: The phase during which both ICN and IP work together before ICN fully replaces IP.**

**Problem with IP:**

1. **Massive Growth of Connected Devices: IPV4 replaced with IPV6. However the trasition is slow as most networks still use NAT**
2. **Internet Usage: most of the traffic comes from content distribution like video or stream, IP don’t mange it efficiently**
3. **HTTP dominance also exposes weaknesses in IP, as earlier there was simple, low bandwidth service when IP was made**
4. **Security limitation: origin authentication, data integrity, and data confidentiality are not guaranteed by default**

**Benefit of ICN:**

1. **In-Network Caching: One of ICN’s strongest features is in-network caching. This means that once a user requests a piece of content, the network stores it temporarily at various points (routers, servers) to serve future requests faster.**
2. **Content Security: ICN secures data by signing content at the source. This ensures data integrity and authenticity**
3. **Support multicasting(sending data to many users simultaneously): because data is cached and distributed locally.**
4. Scalability: ICN is more scalable than IP because the demand for content doesn’t overwhelm a single server. Content can be delivered from multiple sources simultaneously
5. ICN is better suited for **delay-tolerant networks** (like in rural areas or space communications), where constant connectivity isn’t guaranteed. By caching content along the route, ICN ensures that data is available even during disruptions.

**NSF\_NIA Paper:**

**Security and Privacy Challenges of Today’s Internet**

1. **Inherent Lack of Security:**
   1. **IP spoofing (where attackers forge IP addresses),**
   2. **Denial of Service (DoS) attacks (which overwhelm a system with traffic),**
   3. **Eavesdropping on data in transit.**
2. **Patchwork of Security Protocols: Over time, various security protocols like IPSec, SSL/TLS, and DNSSEC have been developed and added to the Internet. However, these are often retrofitted solutions that do not fully address the core architectural vulnerabilities.**
3. **Privacy Concerns: The current Internet architecture does not provide any inherent mechanisms to protect user privacy. Data exchanged over IP can be intercepted and tracked.**

**Four Future Internet Architecture (FIA):**

1. **Nebula**
   1. ** Resilience: Nebula focuses heavily on ensuring network resilience by maintaining multiple paths for data transmission, making it difficult for attacks or failures to disrupt the network.**
   2. ** Trustworthy Computing: Nebula aims to create Trustworthy Computing Platforms (TCPs) that ensure the integrity and authenticity of communications. This is crucial in environments where sensitive data is being transmitted.**
   3. ** Cloud Integration: By leveraging cloud resources, Nebula ensures that data and services remain available even during attacks or network failures.**
2. **Named-Data Networking (NDN): NDN shifts the focus of the Internet from host-centric to data-centric networking. Instead of using IP addresses to route packets, NDN routes data based on content names.**
   1. ** Data-Centric Security: NDN secures data itself rather than securing communication channels. Every piece of content is cryptographically signed, ensuring that it can be trusted no matter where it is cached or retrieved.**
   2. ** In-Network Caching for Privacy: NDN’s in-network caching not only improves performance but also helps reduce the exposure of data flows, enhancing privacy by allowing users to retrieve data from multiple locations.**
   3. ** Name-Based Routing: By routing content based on its name, NDN minimizes traffic correlation attacks that can occur when IP addresses are used to track user activity.**
3. **MobilityFirst (MF):** **It focuses on providing reliable communication in networks with high mobility (such as mobile phones and vehicular networks) by using global unique identifiers (GUIDs) for routing instead of IP addresses.**
   1. **Self-Certifying GUIDs: The architecture uses self-certifying public keys tied to GUIDs.** **immune to certain types of attacks, such as spoofing or man-in-the-middle attacks.**
4. **eXpressive Internet Architecture (XIA):** 
   1. ** Flexible Communication Models: XIA aims to provide security across multiple communication models (host-based, content-based, service-based). Each communication model has its own set of security properties, tailored to the specific needs of that model.**
   2. ** Self-Certifying Identifiers (SCIDs): XIA’s use of SCIDs ensures that all network entities (content, services, hosts) are verifiable and accountable, reducing the possibility of impersonation or unauthorized access.**

**PITFALL OF ISP FRIENDLY P2P design Paper:**

**How to Answer the Potential Exam Questions**

1. **Explain the conflict between P2P networks and ISPs. How does interdomain traffic play a role in this conflict?**
   * **P2P networks generate significant interdomain traffic by randomly selecting peers, causing traffic to cross multiple ISPs, which increases backbone traffic and costs for ISPs. ISPs offer flat-rate pricing, so they don’t profit from increased traffic, leading to the conflict.**
2. **What are the potential benefits of locality-aware peer selection in P2P networks?**
   * **Locality-aware peer selection can reduce interdomain traffic by favoring peers within the same ISP or region. This can lower costs for ISPs and potentially improve download speeds by reducing latency and improving network efficiency.**
3. **Describe the four peer selection strategies tested in the paper. Which strategy showed the most promise in reducing interdomain traffic?**
   * **The strategies tested were Random, Latency-based, Same-AS (peers in the same ISP), and Shortest path (fewest ISP boundaries). The Same-AS and Shortest path strategies showed the most promise, reducing interdomain traffic by up to 43% in larger swarms.**
4. **Why did the authors find that locality-aware peer selection could reduce download performance in certain cases?**
   * **Local peers might have lower bandwidth or slower upload speeds, especially in regions with poor infrastructure, leading to slower downloads when prioritizing them over distant, higher-bandwidth peers.**
5. **What impact does locality-aware peer selection have on the structural robustness of P2P networks?**
   * **Locality-aware designs reduce peer diversity, making the network more vulnerable to failures and congestion. If local peers go offline, users have fewer fallback peers, reducing network resilience.**
6. **How do the interests of Tier-1 ISPs differ from smaller ISPs when it comes to interdomain traffic?**
   * **Tier-1 ISPs profit from more interdomain traffic because they charge smaller ISPs for carrying it. In contrast, smaller ISPs benefit from reducing interdomain traffic because they face higher costs for traffic crossing ISP boundaries.**
7. **Why might Tier-1 ISPs resist adopting ISP-friendly P2P designs?**
   * **Tier-1 ISPs may resist ISP-friendly designs because reducing interdomain traffic would reduce their profits from transit fees charged to smaller ISPs.**
8. **What were the limitations of the Ono plugin in reducing interdomain traffic?**
   * **Ono reduced interdomain traffic by less than 1% in practice. Its effectiveness was limited because client-only solutions don’t have enough control over network-wide traffic patterns, and local peers weren’t always the best-performing ones.**
9. **How does the paper suggest P2P systems could be modified to better balance the interests of ISPs and users?**
   * **The paper suggests that ISP cooperation is necessary for significant reductions in traffic. Solutions like P4P, which involve active ISP guidance for peer selection, can help balance the interests of ISPs and users.**
10. **What are the practical challenges of implementing ISP-friendly P2P designs, according to the study?**
    * **The main challenges include regional performance variations, conflicting ISP interests (especially from Tier-1 ISPs), and the reduction in network robustness due to locality-focused peer selection.**

**SDN\_DDOS:**

**Potential Exam Questions:**

1. **Explain how DDoS attacks exploit weaknesses in network infrastructure.**
   * **DDoS attacks overwhelm network resources like bandwidth, CPU, or memory, rendering the system unavailable for legitimate users. SDN introduces vulnerabilities due to its centralized controller, which can become a target.**
2. **What are the two main categories of DDoS attacks, and how do they differ?**
   * **Transport/Network-level attacks target network protocols (e.g., TCP/UDP), exhausting bandwidth, while Application-level attacks overwhelm server resources by generating excessive requests to applications.**
3. **Describe the CuSum method and its role in DDoS detection.**
   * **CuSum is an anomaly detection method that tracks the deviation of traffic from historical averages. When the deviation exceeds a threshold, it flags a potential DDoS attack. This method is lightweight and adaptive to network conditions.**
4. **Why is an adaptive threshold necessary in the CuSum-based detection method?**
   * **A static threshold might lead to false alarms during peak traffic periods. An adaptive threshold adjusts to real-time traffic conditions, minimizing false positives and maintaining accuracy.**
5. **What types of attacks were used to evaluate the framework, and how were they generated?**
   * **Attacks such as Smurf, Neptune, IPsweep, and Portscan were simulated using CAIDA and DARPA datasets in the Mininet environment. These represent various network and transport-layer DDoS attacks.**
6. **How does the separation of control and data planes in SDN contribute to network vulnerabilities?**
   * **The SDN architecture introduces a centralized controller, which becomes a single point of failure. Attackers can generate excessive control messages (e.g., Packet In), overloading the controller and disrupting network operations.**
7. **Discuss the advantages and limitations of signature-based vs. anomaly-based DDoS detection techniques.**
   * **Signature-based detection is effective for known attacks but fails against new attacks. Anomaly-based detection can catch novel attacks by detecting deviations from normal behavior but often generates false alarms.**
8. **What are the limitations of the existing DDoS detection mechanisms, and how does this paper address them?**
   * **Existing systems often require infrastructure changes or are attack-specific. The paper proposes a lightweight, adaptive solution that can detect a variety of attacks without significant infrastructure modifications.**
9. **What were the key findings regarding the detection rate, false alarm rate, and detection time in the experiments?**
   * **The framework achieved a 100% detection rate, a false alarm rate of 11.63%, and an average detection time of 4.15 seconds, demonstrating both high accuracy and real-time capabilities.**
10. **What future improvements do the authors propose for their DDoS detection framework?**
    * **The authors propose building an automatic mitigation system and extending the framework for multi-domain SDN networks with multiple controllers to further enhance detection and mitigation.**
11. **Explain the complete proposed approach for detecting DDoS attacks in SDN networks.**
    * **The authors propose a CuSum-based anomaly detection framework to monitor traffic deviations. The system computes the cumulative deviation of traffic volume from its historical average and flags potential attacks when this deviation exceeds an adaptive threshold. The adaptive threshold mechanism allows the system to adjust to real-time traffic conditions, reducing false alarms and making it more effective in varying network conditions. The proposed approach is lightweight, does not require major infrastructure changes, and is suitable for real-time DDoS detection.**

**SDN\_ELBA**

**This paper presents ELBA (Efficient Layer-Based Routing Algorithm), a new method for scalable video streaming over Software-Defined Networking (SDN). The goal is to improve the Quality of Experience (QoE) for end users by routing different layers of scalable video content over suitable network paths. The focus is on the H.264/SVC video coding standard, which includes a base layer and enhancement layers that can be streamed with varying levels of quality. The base layer is crucial, as it provides basic video quality, while the enhancement layers improve quality further. By leveraging SDN's programmable control plane, the paper proposes routing algorithms that can adaptively assign different paths to different video layers based on network conditions.**

**Potential Exam Questions:**

1. **What is the main goal of ELBA, and how does it differ from traditional routing algorithms?**
   * **The main goal of ELBA is to enhance video streaming quality in SDN by routing different video layers over different network paths based on their specific Quality of Service (QoS) needs. Unlike traditional algorithms, which route all traffic over a single best-effort path, ELBA uses multiple paths—prioritizing the base layer (for stable quality) over enhancement layers (for improved video quality), thus optimizing both loss and delay for each type of traffic.**
2. **Explain the concept of H.264/SVC video coding and its importance in ELBA's approach.**
   * **H.264/SVC (Scalable Video Coding) divides video into a base layer (providing essential quality) and several enhancement layers (improving resolution, frame rate, or bitrate). ELBA leverages this structure by routing the base layer over highly reliable paths with minimal packet loss, ensuring continuous playback, while enhancement layers, which tolerate more loss, are sent over paths with lower latency, thus dynamically optimizing the network for better video quality.**
3. **How does ELBA utilize SDN's dynamic re-routing capabilities for video streaming?**
   * **ELBA leverages SDN's programmable control plane to dynamically assign different network paths to different video layers based on real-time network conditions. The SDN controller continually monitors network states (e.g., delay, packet loss) and reconfigures routes to ensure that the base layer of the video always uses the most reliable path, while enhancement layers use paths that offer faster delivery, ensuring smooth streaming for users.**
4. **What modifications were made to Dijkstra's algorithm in ELBA, and why?**
   * **In ELBA, Dijkstra’s algorithm is modified to assign edge weights based on both packet loss probability and network delay. This change ensures that the routing decision for the base layer prioritizes low-loss paths, while enhancement layers prioritize low-delay paths. The modification is crucial because it allows the routing algorithm to adapt to the specific QoS needs of different video layers, which was not possible with the standard shortest-path routing algorithm.**
5. **Describe the role of flow-timeouts in ELBA's system architecture.**
   * **Flow-timeouts are used to control the lifecycle of flow entries in SDN switches. In ELBA, IDLE TIMEOUTS are used to ensure that video-related flows (base and enhancement layers) persist as long as the video is streaming, while HARD TIMEOUTS are used for best-effort and background traffic, ensuring that these flows are periodically refreshed. This mechanism ensures that video streams maintain quality and avoid interruptions, while background traffic doesn’t unnecessarily occupy network resources.**
6. **What are the key performance metrics used to evaluate ELBA, and how does it improve video streaming?**
   * **The key performance metrics are PSNR (Peak Signal-to-Noise Ratio) for video quality, frame loss rate, and throughput. ELBA shows a significant improvement in PSNR values for video frames, ensuring clearer and higher-quality video playback. It also reduces the frame loss rate, meaning fewer video frames are dropped, resulting in smoother playback. Furthermore, ELBA increases the overall throughput, ensuring that both video traffic and background traffic are handled efficiently without overloading the network.**
7. **Explain how ELBA balances video traffic with background traffic.**
   * **ELBA achieves balance by assigning different priorities to video and background traffic. Video layers are routed on optimal paths that ensure low loss for the base layer and low delay for enhancement layers, while background traffic is routed using a separate bottleneck shortest-path algorithm. This prevents background traffic from interfering with video traffic, ensuring that video quality is maintained even under heavy network load.**
8. **What are the challenges addressed by ELBA in exchanging information between the control plane and streaming servers?**
   * **ELBA introduces a ToS (Type of Service) mapping mechanism that helps communicate the characteristics of different video layers between the SDN controller and the streaming servers. This mechanism allows the controller to prioritize different traffic types without needing to inspect the packet's contents (avoiding the need for deep packet inspection). By identifying the type of video layer, the controller can assign the appropriate path dynamically, which is crucial for real-time adaptive routing.**
9. **What future improvements do the authors suggest for ELBA?**
   * **The authors propose extending ELBA to multi-domain SDN environments, where multiple SDN controllers manage different parts of the network, enabling it to scale across larger networks. They also suggest incorporating additional metrics like jitter (variability in packet arrival times) and congestion to further optimize the QoS for video streaming. These improvements aim to enhance ELBA’s adaptability and effectiveness in more complex and dynamic network conditions.**
10. **How does ELBA ensure that enhancement layers are delivered on time without affecting the base layer's delivery?**

* **ELBA ensures timely delivery of enhancement layers by routing them on low-delay paths, while the base layer, which requires lossless transmission, is routed on low-loss paths. This separation of traffic ensures that enhancement layers are delivered quickly, reducing the likelihood of video buffering or delay, while maintaining the integrity of the base layer’s delivery. This balance is critical for maintaining high video quality and uninterrupted playback for users.**

**SDN\_IXP:**

** What is the significance of combining MTD with SDN at the IXP level in preventing DoS attacks?**

* **Combining Moving Target Defense (MTD) with Software-Defined Networking (SDN) at the Internet Exchange Point (IXP) level provides an innovative way to dynamically reconfigure the network to defend against Denial of Service (DoS) attacks. MTD makes the network more resilient by changing network parameters like IP addresses, making it difficult for attackers to predict network configurations. SDN, with its centralized control, enables the dynamic routing and reconfiguration necessary to apply MTD strategies in real time at a critical network juncture like the IXP, where multiple Autonomous Systems (AS) connect. Together, these strategies increase network security by minimizing attack surfaces and reacting quickly to threats.**

** How does the random host-IP mutation technique work in the proposed framework, and what role does it play in enhancing security?**

* **The random host-IP mutation technique regularly changes the virtual IP addresses of hosts. The real IP address is retained internally within the network, while the externally exposed virtual IP addresses are dynamically altered by the SDN controller. This technique prevents attackers from easily targeting specific hosts because, by the time an attacker identifies a virtual IP, it may have already been mutated. The SDN controller maintains a mapping between virtual and real IPs and updates this mapping periodically or based on traffic patterns. This makes it difficult for attackers to perform successful reconnaissance or launch targeted attacks, thus enhancing security.**

** Explain the role of the SDN controller in managing network traffic and detecting DoS attacks in this framework.**

* **The SDN controller serves as the central decision-making entity in the proposed framework. It dynamically manages network traffic by installing, updating, and removing flow rules for forwarding packets. The SDN controller also continuously monitors traffic statistics across the network to detect any anomalous behavior, such as a sudden spike in packet rates that could indicate a DoS attack. Using techniques like change-point detection and Exponentially Weighted Moving Average (EWMA) analysis, the controller can identify suspicious traffic patterns. Upon detecting abnormal traffic, the controller can immediately mitigate the threat by installing DROP rules to block malicious flows, thus preventing attacks from overwhelming the network.**

** What is the role of Exponentially Weighted Moving Average (EWMA) in detecting DoS attacks, and how does it work?**

* **EWMA is used in this framework as a traffic analysis tool to detect deviations from normal network behavior. It continuously monitors packet arrival rates and calculates a weighted average that emphasizes more recent data, allowing the system to quickly detect sudden spikes in traffic. When the observed traffic deviates significantly from the expected traffic pattern (as determined by the EWMA), it may signal a DoS attack. The SDN controller uses this information to assess whether the traffic is normal or malicious. By identifying such deviations early, the EWMA method helps prevent attacks from escalating and affecting legitimate traffic.**

** Describe the experiment setup used for evaluating the proposed framework. What tools and datasets were used?**

* **The authors set up an emulation environment using MiniNext, which is an extension of Mininet that includes advanced network capabilities, to simulate a real-world network scenario involving three Autonomous Systems (ASs) connected via an SD-IXP switch. The network emulation involved both Nmap scans to test reconnaissance defense and datasets such as CAIDA and DARPA intrusion detection datasets to simulate DoS attacks. These datasets contain real-world network traffic, including both legitimate and attack traffic, allowing the authors to evaluate the effectiveness of the host-IP mutation and DoS detection mechanisms under realistic conditions.**

** What were the key findings from the evaluation of the framework, specifically regarding reconnaissance blocking and DoS detection?**

* **The evaluation of the proposed framework showed that it successfully blocked a significant portion of network reconnaissance attempts. Only 16% of aggressive Nmap scans succeeded, demonstrating the effectiveness of the host-IP mutation scheme in protecting against reconnaissance. In terms of DoS detection, the framework achieved a Detection Rate (DR) close to 100% for most attack types, meaning that it was able to identify virtually all DoS attacks. Additionally, the framework exhibited a False Alarm Rate (FAR) as low as 7.1%, indicating that it could differentiate between legitimate and malicious traffic with high accuracy and minimal disruption to normal operations.**

** How does the paper propose to extend the framework for future work, and what areas need further investigation?**

* **For future work, the authors propose extending the framework to address Distributed Denial of Service (DDoS) attacks, where attacks are launched from multiple sources simultaneously, posing a greater challenge. Handling DDoS attacks would require more advanced coordination between the SDN controller and the network infrastructure to block traffic from multiple points. Additionally, the authors plan to test the framework on a physical testbed, rather than relying solely on emulation, to better understand its real-world performance and scalability. Further investigation will also focus on improving detection algorithms to handle more sophisticated and evolving attack strategies.**

** What are the operational overheads associated with the proposed SDN-based host-IP mutation scheme, and how does it impact the network's performance?**

* **The operational overhead introduced by the host-IP mutation scheme includes managing a large pool of IP addresses for mutation and handling the additional computational tasks performed by the SDN controller, such as continuously updating the mappings between real and virtual IPs. However, the paper reports that the overhead on the SDN controller was minimal, with CPU usage increasing by less than 5% during experiments. The mutation scheme also requires sufficient IP address space to generate new virtual IPs regularly, which could pose a limitation in networks with a restricted address pool. Despite these overheads, the framework was shown to perform efficiently without causing noticeable delays or degradation in overall network performance.**

** How does the framework ensure that legitimate connections are not disrupted when IP addresses are changed due to host-IP mutation?**

* **The framework ensures that ongoing legitimate connections are not disrupted by managing the flow rules on the SDN switches. Even after an IP mutation, connections that were already established before the mutation are allowed to continue until their flow rules naturally expire. This approach prevents sudden termination of active connections, maintaining user experience and avoiding any unnecessary reestablishment of sessions. The SDN controller monitors and manages flow expiration times, ensuring that new virtual IPs are only applied to future connections while preserving the integrity of ongoing traffic.**

** Explain the process of network reconnaissance and how the proposed framework mitigates it using host-IP mutation.**

* **Network reconnaissance is the process by which attackers scan a network to identify active hosts, services, and open ports, which can then be exploited in subsequent attacks. Tools like Nmap are commonly used for reconnaissance by sending probe packets and analyzing the responses. The proposed framework mitigates reconnaissance by implementing a host-IP mutation strategy, where the external (virtual) IP addresses of hosts are frequently changed. This dynamic reconfiguration makes it extremely difficult for attackers to accurately map the network or target specific hosts because the virtual IPs they observe during scanning quickly become invalid. The constant changing of IP addresses confounds reconnaissance efforts and helps prevent further exploitation.**

**SDN\_PANORAMA:**

**Potential Exam Questions:**

1. **What is the primary objective of PANORAMA, and how does it differ from traditional network monitoring tools?**
   * **PANORAMA’s main objective is to provide a real-time, lightweight network monitoring solution in Software-Defined Networks (SDN), specifically using the OpenFlow protocol. Unlike traditional monitoring tools, which often require expensive infrastructure changes or active monitoring techniques that inject probe packets (introducing additional traffic), PANORAMA is designed to be non-intrusive. It passively collects flow and port statistics from switches without impacting normal network traffic. This allows for continuous real-time monitoring without additional network overhead, making it ideal for dynamic environments such as SDN.**
2. **Explain the difference between active and passive network monitoring approaches, and where PANORAMA fits into these categories.**
   * **Active monitoring involves injecting probe packets into the network to measure performance metrics such as latency, packet loss, and throughput. While effective, this approach adds overhead by creating additional traffic and can interfere with normal network operations. On the other hand, passive monitoring relies on observing traffic that is already flowing through the network without introducing new packets, thus reducing the monitoring footprint.**
   * **PANORAMA fits into the passive monitoring category as it collects network statistics directly from the switches using OpenFlow PORT STATS and FLOW STATS messages, without introducing extra traffic. This makes it a more scalable and efficient solution compared to traditional active monitoring approaches.**
3. **Describe the role of OpenFlow in PANORAMA’s architecture and its significance for network monitoring.**
   * **OpenFlow is central to PANORAMA’s architecture because it enables communication between the SDN controller and the switches. Through OpenFlow, PANORAMA can collect real-time statistics on network traffic, including per-port and per-flow statistics. OpenFlow also allows PANORAMA to discover network topology, monitor data transfer rates, and evaluate link conditions. The significance of OpenFlow lies in its ability to manage traffic flows dynamically, which gives PANORAMA the ability to efficiently monitor network behavior without modifying the underlying infrastructure. By using OpenFlow, PANORAMA can integrate seamlessly with existing SDN environments and provide a real-time bird’s eye view of the network.**
4. **How does PANORAMA handle link discovery and host discovery in an OpenFlow network, and why are these processes important for network monitoring?**
   * **Link Discovery in PANORAMA is managed using the Link Layer Discovery Protocol (LLDP). The OpenFlow controller sends out LLDP packets to switches, which broadcast them to neighboring switches. When a switch receives an LLDP packet, it informs the controller, allowing PANORAMA to map the physical links between switches, thereby constructing a real-time view of the network topology.**
   * **Host Discovery occurs when a host sends packets through a switch. If the switch does not have an existing flow entry for the packet, it forwards the packet to the controller, which learns the host’s IP address, MAC address, and the associated switch. This process is critical because understanding the network topology and knowing where hosts are located helps PANORAMA monitor network health, troubleshoot issues, and optimize traffic flows.**
5. **What are the key types of statistics collected by PANORAMA, and how do they contribute to real-time network monitoring?**
   * **PANORAMA collects several key types of statistics:**
     + **Port Statistics: These provide insights into the health and performance of individual switch ports, including the number of transmitted and received packets, byte counts, and errors such as packet drops, collisions, or CRC errors. Monitoring port statistics helps detect issues like port congestion, faulty links, or hardware failures.**
     + **Aggregate Statistics: These reflect the overall traffic processed by each switch, including the total number of flows, packets, and bytes. Aggregate statistics are essential for monitoring network load and identifying areas of high traffic that may become bottlenecks.**
     + **Flow Statistics: PANORAMA collects details on each flow, including flow match fields (like source/destination IP addresses, TCP/UDP ports), packet counters, and timeouts. This granular data helps network administrators monitor specific traffic flows and ensure critical flows are prioritized.**
   * **By collecting these diverse statistics, PANORAMA offers a comprehensive view of both high-level and granular network activity, helping to detect performance degradation, troubleshoot issues, and optimize network operations.**
6. **How does PANORAMA calculate the data transfer rate (DTR) of a link, and why is this metric important for network monitoring?**
   * **PANORAMA calculates the Data Transfer Rate (DTR) by analyzing the number of bytes transmitted and received on each port over a period of time. DTR can be calculated for both unidirectional and bidirectional traffic flows. By regularly querying the OpenFlow switches for port statistics, PANORAMA can compute the DTR in real-time.**
   * **The importance of DTR lies in its ability to reveal the bandwidth utilization of network links. High DTR values may indicate links that are approaching or exceeding capacity, while low DTR values can help identify underutilized resources. Monitoring DTR is crucial for detecting bottlenecks, optimizing traffic routing, and ensuring efficient bandwidth usage across the network.**
7. **What were the key findings from PANORAMA’s experimental evaluation, and how did it perform in both physical and emulation environments?**
   * **The experimental evaluation of PANORAMA was conducted in both a physical testbed and an emulated environment using Mininet. The key findings include:**
     + **Topology Discovery: PANORAMA successfully discovered the network topology, identifying the physical links between switches in real-time using LLDP.**
     + **Port and Flow Statistics: The tool accurately collected port and flow statistics, which were verified against OpenFlow tools like dpctl, confirming the accuracy and reliability of PANORAMA’s data collection.**
     + **Data Transfer Rate (DTR): PANORAMA’s calculation of DTR between switches provided useful insights into the network's bandwidth utilization, allowing for the detection of potential bottlenecks.**
   * **Overall, PANORAMA performed well in both test environments, showing its effectiveness in real-time monitoring while imposing minimal computational overhead.**
8. **What future improvements do the authors suggest for PANORAMA, and how do they plan to extend its functionality?**
   * **The authors suggest several improvements for future versions of PANORAMA:**
     + **Incorporation of Additional Metrics: Future versions of PANORAMA will include monitoring metrics such as network congestion, jitter, and other performance indicators. These metrics will provide a more comprehensive view of network conditions, particularly for applications sensitive to latency and delay variation, such as real-time video streaming.**
     + **Controller Independence: Currently implemented as a POX module, the authors plan to develop PANORAMA as a controller-independent tool, making it compatible with other popular SDN controllers like OpenDaylight or ONOS. This would increase PANORAMA’s versatility and wider adoption across different SDN platforms.**
     + **Graphical User Interface (GUI) Enhancements: Enhancements to the GUI will allow network administrators to visualize link loss, delay, and other key performance indicators (KPIs) in real-time, making it easier to monitor network health and diagnose problems.**

**SKYPE**

**Potential Exam Questions (Expanded and Detailed):**

1. **What are the two types of nodes in Skype’s peer-to-peer architecture, and how do they function?**
   * **Skype’s network consists of two main types of nodes:**
     + **Ordinary Hosts (OHs): These are regular Skype clients installed on users’ computers. They initiate and receive calls and messages. Ordinary hosts rely on other nodes in the network to help with NAT traversal, call routing, and establishing connections when direct peer-to-peer communication is not possible due to network constraints like firewalls.**
     + **Super Nodes (SNs): These are more powerful nodes with public IP addresses, sufficient CPU, memory, and bandwidth to handle additional networking tasks. Super Nodes help relay traffic, particularly for clients behind NATs or firewalls. They perform critical tasks such as assisting in call establishment, managing host caches, and maintaining connectivity in the peer-to-peer network.**
   * **Functionality: Super Nodes act as intermediaries when direct communication between two clients isn’t possible. They help form the backbone of the Skype network, enabling robust and scalable communication without needing centralized servers (except for the login process).**
2. **Describe the login process in Skype. What role does the login server play, and how does Skype maintain reliability during this process?**
   * **Login Process: When a user launches Skype, the client (ordinary host) attempts to connect to a Super Node. The client sends encrypted credentials (username and password) to the Super Node, which then forwards the credentials to the centralized Skype login server for authentication.**
     + **If the central login server is available, it verifies the credentials and returns a response, allowing the user to access their buddy list and start using the Skype network.**
     + **If the login server is temporarily unreachable, Skype retries the process by connecting through other available Super Nodes.**
   * **Role of the Login Server: The login server is the only centralized component in the Skype architecture. It handles:**
     + **User authentication (ensuring correct login credentials).**
     + **Synchronization of buddy lists and other account-related data.**
     + **Managing username uniqueness and credentials across the global network.**
   * **Reliability: Skype uses its distributed P2P network to ensure that even if a direct connection to the login server fails, users can still log in by rerouting through Super Nodes, making the login process more resilient and fault-tolerant.**
3. **How does Skype handle NAT and firewall traversal, and why is this important for ensuring connectivity across different network environments?**
   * **NAT and Firewall Traversal: Many VoIP clients face difficulties when operating behind Network Address Translators (NATs) and firewalls, which block direct communication between devices by translating private IP addresses to public ones. Skype overcomes these challenges using several techniques:**
     + **STUN-like Techniques: Skype uses techniques similar to STUN (Session Traversal Utilities for NAT), which helps clients discover their public IP addresses and the nature of the NAT device they are behind. This helps in determining the best communication method (e.g., direct peer-to-peer or relayed via a Super Node).**
     + **TURN-like Mechanism: When both communicating parties are behind restrictive firewalls or NATs, Skype uses Super Nodes as relays. This ensures that even if a direct peer-to-peer connection cannot be established, communication is still possible by routing through an intermediary node.**
     + **Dynamic Port Selection: Skype uses randomly selected ports for both UDP and TCP communication, bypassing the typical port restrictions set by firewalls.**
   * **Importance: NAT traversal is crucial for ensuring that Skype functions seamlessly across different network environments, from corporate networks with stringent firewalls to home routers using NAT. Without these techniques, many users would be unable to establish calls or send messages.**
4. **What codecs does Skype use for voice calls, and why are they significant for maintaining high voice quality even in low-bandwidth scenarios?**
   * **Skype uses several audio codecs optimized for wideband audio and efficient voice communication:**
     + **iLBC (Internet Low Bitrate Codec): Designed to handle packet loss effectively, iLBC is used for low-bandwidth situations while maintaining acceptable voice quality.**
     + **iSAC (Internet Speech Audio Codec): This codec adapts to network conditions and can scale its bitrate based on available bandwidth, making it ideal for variable network environments.**
     + **iPCM (Internet Pulse Code Modulation): A higher bitrate codec that provides excellent voice quality but requires more bandwidth.**
   * **Significance: These codecs are essential for maintaining high-quality voice communication, even under poor network conditions with limited bandwidth (as low as 32 kbps). The ability to dynamically switch between codecs and adjust to network conditions allows Skype to offer superior voice quality compared to many other VoIP services.**
5. **Explain the role of Super Nodes in the Skype network. How are they selected, and what specific tasks do they perform?**
   * **Super Nodes (SNs) play a crucial role in maintaining the functionality and scalability of the Skype network. They are chosen based on their network resources, such as having a public IP address, sufficient CPU power, memory, and bandwidth. Super Nodes are responsible for:**
     + **Routing traffic between ordinary hosts, particularly for clients behind NATs or firewalls.**
     + **Relaying communication when direct peer-to-peer connections cannot be established.**
     + **Maintaining host caches that store IP addresses of other nodes, ensuring that Skype clients can always find available Super Nodes to connect to.**
     + **Assisting with login processes by connecting clients to the centralized login server.**
   * **Selection Criteria: Skype dynamically promotes certain clients to Super Nodes based on their resources and connectivity. Nodes that meet the necessary conditions (public IP, high bandwidth, etc.) may automatically become Super Nodes, helping to distribute the workload across the network.**
6. **How does Skype ensure security during calls and messaging, and what encryption techniques does it employ?**
   * **Skype prioritizes end-to-end encryption for both calls and messaging, ensuring that communication between users remains private and secure. The security model involves:**
     + **AES-256 Encryption: All voice, video, and text data are encrypted using Advanced Encryption Standard (AES-256), providing strong protection against unauthorized access.**
     + **RSA Encryption: Skype uses RSA-1024 or RSA-2048 for key exchange. RSA ensures that encryption keys are exchanged securely between clients, preventing man-in-the-middle attacks.**
     + **Digital Signatures: Each client has a unique digital certificate issued by the Skype login server, which is used for authentication and verifying the identity of communication participants.**
   * **Why It Matters: These encryption techniques ensure that Skype users are protected against eavesdropping, unauthorized access, and tampering, making it one of the most secure VoIP services available.**
7. **What are the advantages of using a peer-to-peer (P2P) architecture in Skype compared to a client-server model, particularly in terms of scalability and reliability?**
   * **Advantages of P2P Architecture:**
     + **Scalability: Unlike traditional client-server models, which rely on centralized servers to handle communication, Skype’s P2P architecture distributes the workload across all connected nodes. This means the system can scale easily as more users join the network, without overloading any single server.**
     + **Reduced Centralized Infrastructure: P2P minimizes reliance on costly centralized servers. The only central element in Skype’s architecture is the login server; once authenticated, users communicate directly with each other or via Super Nodes, reducing dependency on central infrastructure.**
     + **Increased Reliability: Since there is no single point of failure, Skype remains operational even if several nodes or Super Nodes go offline. Communication routes can be dynamically reconfigured to maintain connectivity, making Skype highly fault-tolerant.**
8. **How does Skype handle call establishment between two clients that are both behind NATs or firewalls?**
   * **NAT Traversal for Call Establishment: When both clients are behind NATs or firewalls, Skype uses a combination of techniques to establish the call:**
     + **UDP Punching: If possible, Skype tries to establish a direct UDP connection by sending packets through NAT devices, hoping that the NAT will allow the connection.**
     + **Super Node Relaying: If direct communication is not possible, Skype uses Super Nodes to relay the call. The Super Node acts as an intermediary, forwarding traffic between the two clients.**
     + **Fallback to TCP: If neither UDP nor direct connections are feasible, Skype falls back to TCP, using the Super Node to route traffic. While this method introduces more latency, it ensures that the call can still be established.**
   * **Why It’s Important: These strategies allow Skype to connect users in almost any network environment, ensuring that users behind NATs or firewalls can still make calls seamlessly.**
9. **What is the significance of Host Cache in Skype, and how does it contribute to network resilience and connectivity?**
   * **Host Cache is a list of known Super Nodes and their IP addresses, which is stored on each Skype client. The host cache allows clients to quickly connect to the network, even after being offline or when other nodes are unavailable. Skype updates the host cache periodically to ensure that the client can always find an active Super Node.**
   * **Contribution to Resilience:**
     + **Ensures Connectivity: If a Super Node becomes unreachable, the client can try other Super Nodes from its host cache, ensuring that the user remains connected to the network.**
     + **Reduces Reliance on Central Servers: The host cache minimizes the need for continuous connections to central servers by allowing clients to autonomously find Super Nodes, improving network scalability and fault tolerance.**
10. **Compare Skype’s performance in terms of latency and memory usage with other instant messaging and VoIP clients like Yahoo, MSN, and Google Talk.**
    * **In terms of performance, Skype has been found to offer superior latency and memory management compared to competitors like Yahoo Messenger, MSN, and Google Talk.**
    * **Latency: Skype exhibits the lowest mouth-to-ear latency (approximately 96 ms), which is a key factor in maintaining high voice quality during calls. This latency is significantly better than Yahoo (152 ms), MSN (184 ms), and Google Talk (109 ms), making Skype the preferred choice for real-time communication.**
    * **Memory Usage: Skype optimizes its resource usage by adjusting its process priority during calls. This ensures that calls are not disrupted by other background processes on the host machine, resulting in a smoother experience compared to other VoIP services, which may not prioritize calls in the same way.**