128 TECHNOLOGY

FEATURE BRIEF: OVERLAPPING IP ADDRESSES

Introduction

Private networks use the private IP address space. The IPv4 and IPv6 specifications define private address ranges. These addresses are used for local area networks (LANs) in residential, office, and enterprise environments. Different enterprises or different locations within the same enterprise may use the same IP address range. Private IP addresses are not allocated to any organization and anyone may use these addresses. However, IP packets addressed from them cannot be routed through the public Internet.

Overlapping IP addresses result when you assign an IP address to a device on the network that is already assigned to a device on the Internet or outside network. Overlapping IP addresses also occur when networks are merged after corporate acquisitions. These networks must be able to communicate without having to readdress all their devices.

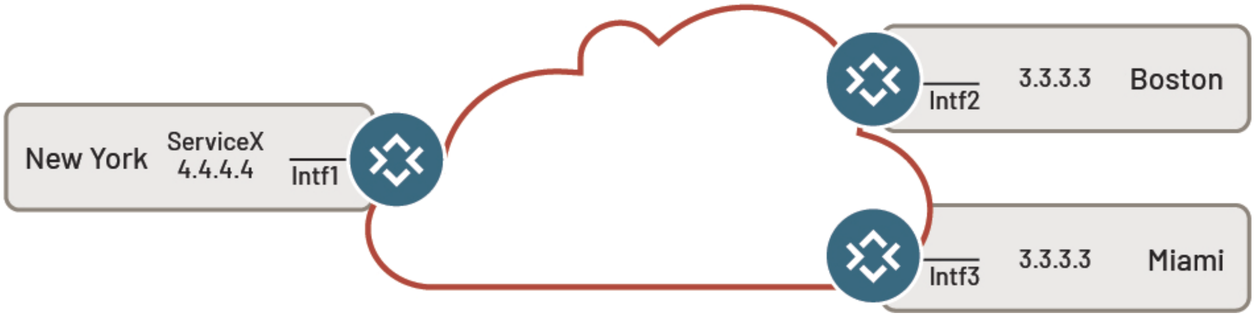
Another scenario where overlapping IP addresses space is an issue is when multiple customers with overlapping IP addresses are managed or offered services from a common data center. For example, a managed service provider (MSP) may have multiple customers who have overlapping IP addresses connecting to a common collaboration solution hosted at a common data center.

128 Technology Session Smart™ Routers inherently solve overlapping IP address range issues with Secure Vector Routing (SVR).

SVR inherently masquerades internal IP addresses by hiding an entire IP address space, usually consisting of private IP addresses, behind a single IP address in another, usually public address space. This allows for communication between two sites with overlapping IP addresses belonging to the same enterprise or those belonging to different enterprises to communicate with a common service residing in a data center. SVR along with the ability to use words to describe services and tenants makes it a perfect solution for overlapping IP addresses.

Deployment

Overlapping IP addresses become a challenge when two sites using the same private addresses need to communicate with a common data center. In this case there is no way for the data center to distinguish between the branches.



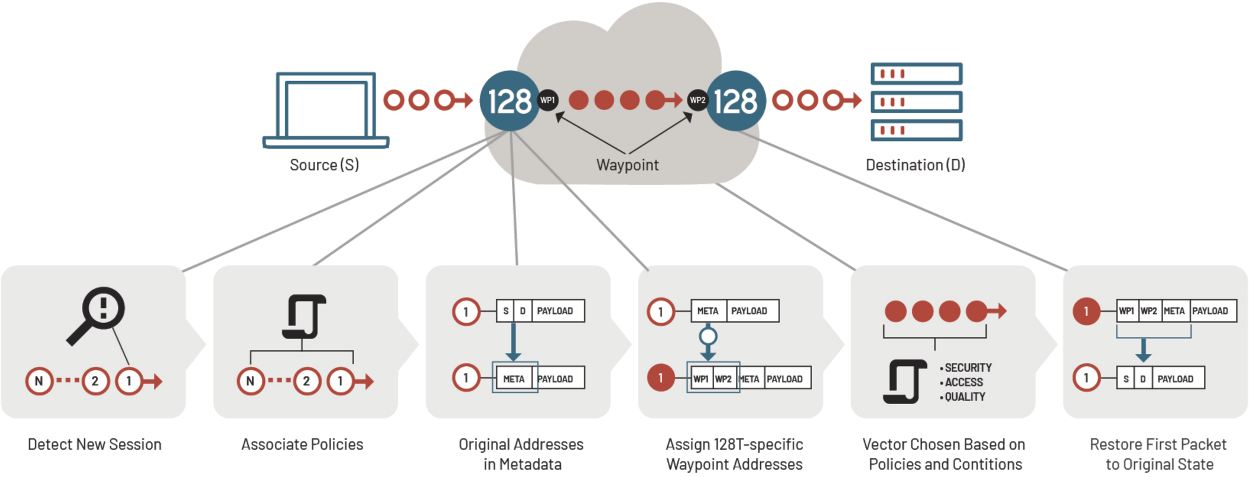
This deployment scenario is common when branches belonging to the same enterprise or different enterprises access the same service located at a common data center. Assume a service X is hosted in a data center located in New York. There are two branches located in Boston and Miami with overlapping IP addresses belonging to two different enterprises that need to access this service.

128T Session Smart Routers are service-oriented and forward packets towards named services. These services can be learned by the 128T Session Smart Routers via configuration, through the management tool dynamically, or via DNS. In our example, the Boston and Miami routers have learned that Service X is accessible via the New York router. The 128T Session Smart Routers use SVR to communicate between hosts located in the branches and the service located in the data center.

When a host in Boston sends packets to establish a session with the Service in New York – a SVR connection is established between the 128T Session Smart Routers in Boston and New York.

The first packet of each session serves to establish an end-to-end path across the network, defining waypoints based on the 128T Session Smart Routers it crosses along the way. It also initiates a single end-to-end session from ingress to egress that is transient in nature. The remaining packets that are part of the session are sent along the same path without any tunnel overhead.

When the first packet corresponding to a new TCP or UDP session arrives at the 128T Session Smart Router in Boston, it determines the appropriate route corresponding to the session. If a route is found:



- The 128T Session Smart™ Router translates the source address of the packet to its own egress waypoint IP address. The destination address of the packet is translated to the waypoint address of the destination SVR-based router. Unique source and destination ports are also selected. In cases without overlapping IP addresses, the original source address, destination address, protocol, source port, and destination port (original 5 tuple) serve as a means to uniquely identify the session.

In this scenario, both Boston and Miami sites have the same IP addresses and they want to a reach a service in New York. The 5 tuples will be the same for sessions from both sites. In this case a sixth field which is the router peer ID is added to make a 6 tuple. When packets from Boston and Miami arrive at New York – the 6 tuple helps to uniquely identify packets from different sites or customer groups with overlapping IP addresses.

- The Boston router adds metadata to the packet. This metadata includes unique 6 tuple, along with other policy and control parameters. The metadata is then signed and optionally encrypted based on policy.
- The packet is then forwarded to the waypoint address of the next secure vector router. All routers along the path forward these packets as any regular packet.
- At the New York router, once authenticated and authorized, the original packet contents are restored, and it's forwarded to the final destination.
- Subsequent packets from the same session are automatically recognized and forwarded in the same way, but without "first packet processing".
- Similar to above processing, SVR adds metadata to the first reverse packet, which follows the same path as the first forward packet. Now, complete path symmetry is established.

The router in New York must source-NAT the packets. This is needed because though the 128T Session Smart™ Routers can handle overlapping IP addresses, the server at the destination IP address will not be able to distinguish between packets coming from two different sites with the same 5 tuples. Source-NAT must be enabled on the egress interface Intf1 of the 128T Session Smart Router in New York so that the server can identify sessions from Boston and Miami as different sessions.

By carefully coordinating source and destination address translations, the 128T Session Smart Routers enable access to services in situations with addresses overlap.

Summary

With corporate mergers, branch office consolidations, and partner collaborations becoming common, often an enterprise will have sites that use the same private address subnets. It is also common for organizations with large number of branch sites to utilize the same private addresses in every branch to simplify the deployment. 128T Session Smart™ Routers can handle overlapping IP addresses seamlessly by utilizing SVR. There are no complex virtualization techniques to configure per router making it the ideal solution for overlapping IP addresses.