Kate Moreland

kem0149

COMP 4320: Assignment 5

**Problem 1:**

Imagine you are an experienced network engineer responsible for designing a future-proof network infrastructure that supports both IPv4 and IPv6, efficient routing mechanisms, and modern control plane architectures. Using your understanding of IPv6 transition strategies, routing algorithms (Dijkstra’s algorithm, Link-State and Distance-Vector), and SDN, answer the following questions:

**1.1 Explain the primary motivations behind IPv6 adoption, including the limitations of IPv4. Describe the key differences between IPv4 and IPv6, including addressing, packet structure, and header simplifications. Discuss two major transitions strategies (Tunneling and Dual Stack) and explain how IPv6 packets can be transmitted over an IPv4-only network.**

IPv6 was primarily made to fix the issues that come with IPv4. These are address exhaustion, inefficient routing and NAT complexity, security issues, and increased want for IoT and mobile devices. Address exhaustion is shown in IPv4 because it only provides 4.3 billion unique address which is nowhere near enough. Inefficient routing and NAT complexity in IPv4 is because it mainly uses NAT which makes peer-to-peer communication difficult and keeps it small. Security issues arise with IPv4 due to the fact that it does not support IPsec. The increased demand for IoT and mobile devices need a more scalable network which cannot be accomplished with IPv4. IPv6 has an address length of 128-bits and IPv4 only has 32-bit. The header complexity is much simpler with a certain 40-byte base header, while IPv4 is all over the place with optional fields. The header fields only have 8 fields and IPv4 has 13. The NAT usage is not necessary due to the fact that each and every device has an unique address, but IPv4 is much more usual because of the small address area. IPsec in IPv6 is necessary, while in IPv4 is it your choice. The idea of tunneling is to make sure that IPv6 packets can only be sent on an IPv4 based infrastructure. It works through encapsulating IPv6 packets on the inside of IPv4 packets. This can be accomplished through the use of 6to4 or ISATAP. Tunneling can be very helpful in the early development phase of IPv6 in networks where not all of the functions of IPv6 are in effect quite yet. Dual stack is used to make sure systems can run both IPv4 and IPv6 at the same time. This is accomplished through having all devices designed in both IPv4 and IPv6 and then based on what is available and needed then choosing what to use. Dual stack helps with a change from IPv4 to IPv6 over a longer period of time and enables using IPv4 to look back.

**1.2 Compare Link-State and Distance-Vector routing algorithms, explaining how each determines the shortest path. Explain the working of Dijkstra’s Algorithm in a Link-State routing environment and discuss its advantages over Distance-Vector approaches. Discuss scalability issues in these algorithms and how they handle dynamic network changes.**

The Distance-Vector starts with only having knowledge of its neighbors. The routing updates are periodic. The convergence speed is much slower because it can result in loops. An example of an algorithm is RIP. The path calculation is given through the Bellman-Ford algorithm. The Link-State starts with a complete view of the whole network. The routing updates are only done with events and only the changes are shown. The convergence speed is faster compared to the Distance-Vector because the whole map is already completed. An example of an algorithm is OSPF. The path calculation is given through the Dijkstra’s algorithm. Dijkstra’s algorithm in Link-State routing beings by every router completing a Link-State database by getting the Link-State advertisements from the surrounding states. Then, the Dijkstra’s algorithm is able to calculate the shortest path from the starting state top all of the states. Finally, the routing tables are found by the shortest path. The advantages of this approach are that it avoids the loops which slow it down. It also takes the best path selection by showing all of the options. When there is a large hierarchical network Link-State is much better and more efficient. Distance-Vector struggles with the concept of scalability because it is not able to see everything and only certain updates. Distance-Vector is very slow to identity any errors and loops occur often. Link-State has the ability to change quickly through the idea of LSA flooding. It also is able to compute SPT in a timely manner.

**1.3 Explain the difference between a traditional per-route control plane and a logically centralized SDN control plane. Discuss how OpenFlow enables SDN, including the role of flow tables, match-action rules, and SDN controllers. Analyze how SDN improves SDN network efficiency and flexibility, particularly in large-scale enterprise and cloud environments.**

A traditional network is spread out in every router. You are also able to configure and change a traditional network in each device. The policies that are implemented are static and implemented for a single device. The SDN are much more centralized and located logically through the SDN controller. The configuration is able to be programmed and managed globally by a controller again. The policies are dynamic and are implemented all throughout the network. The parts of the OpenFlow are switches, flow table entries, and SDN controller. The switches are able to keep the flow tables with entries. The flow table entries have the ability to identify the fields, do different actions, control priorities, and implement counters. The SDN controller is able to decide and implement rules onto the switches using OpenFlow protocol. SDN is able to have a centralized network intelligence by making the policies quite simple and creating a simpler troubleshoot process and identifying the errors. The ability to have programmability and automation allows for dynamic path calculation and monitors intent-based networking. The ability to have scalability and flexibility it created a central logic help multi-tenant and cloud-scale models. It is also perfect for NFV. The security aspect is shown through the global visibility. It also works with micro segmentation.

**Problem 2:**

As a network architect, you are responsible for designing a scalable, efficient, and policy-driven routing architecture for a large service provider network. Using your understand of distance-vector algorithms (Bellman-Ford), link-state algorithms (Dijkstra's Algorithm), intra-AS routing (OSPF, RIP), inter-AS routing (BGP), and policy-based routing, answer the following questions:

**2.1 Describe the differences between intra-AS and inter-AS routing, explaining why different routing protocols are used within an AS (RIP, OSPF) versus across ASes (BGP). Explain how BGP (Border Gateway Protocol) propagates reachability information using eBGP and iBGP. Discuss BGP path attributes (AS-PATH, NEXT-HOP, LOCAL\_PREF) and how they influence route selection.**

The intra-AS routing is in one autonomous system. It takes use of the protocols RIP, ISPF, EIGRP, IS-IS. The trust model is trust exist which is only one administrative domain. The routing goal is to take use of the optimal path choices and very quickly meets. The algorithm type is usually Link-State or Distance-Vector. The inter-AS routing is in-between many different ASes. The protocols that are in use are BGP. There is no trust because each policy can be different per AS. The routing goal is policy motivated path control. The algorithm type is Path-Vector. The eBGP, which is the external BGP, is able to attach routers in different ASes. It also shows that advertisements are delivered along with AS-PATH modifications. It usually takes advantage of neighbors that are interlocked. The iBGP, which is the internal BGP, is able to attach router in the same AS. It does not change the AS-PATH. It needs a neighbor that is directly connected. The AS-PATH is a list of Asesa route has traveled. It is also used to stop loops from occurring and take advantage of a shorter path. The NEXT-HOP is next-hop router’s IP address. It makes sure that is dependable and effects the next-hop choice. The LOCAL\_PREF is used to show routes in an AS. The impact on the routing decision is the higher is the better. It is useful for exiting traffic control.

**2.2 Describe how BGP policy controls inter-AS routing decisions, prioritizing paths based on AS relationships (provider, peer, customer). Explain the hot potato routing strategy, where ISPs forward traffic to the closest AS exit point to minimize transit costs. Given a scenario where an AS wants to avoid routing transit traffic while ensuring redundancy, propose an optimal routing policy using BGP attributes.**

BGP grants the fine-grained policy enforcement by taking use of route filtering. The decisions are made by the AS relationships. The customer purchases the AS for the ability to connect. This is preferred. The peer takes part in transaction free exchange of traffic. This is in the middle of preference. The provider raises the price for the AS for any upstream access and this is not at all preferred. The hot potato routing is when an ISP transitions traffic to the following AS as soon as available so it will minimize any cost. It takes use of IGP metrics to make to the closest egress point. This can end up in suboptimal end-to-end paths that is used for the user but it also makes sure the cost is low for ISP. An example of a traffic avoidance can be seen when an AS wishes to keep up a connection with multiple providers. It also wants to keep away from becoming a transit AS. This also makes sure that both incoming and outgoing traffic will follow the original intent. My idea of an optimal routing policy can begin with setting LOCAL\_PREF. It also fails to advertise. It takes use of the BGP communities. It uses the inbound filters and out-of-band monitoring.

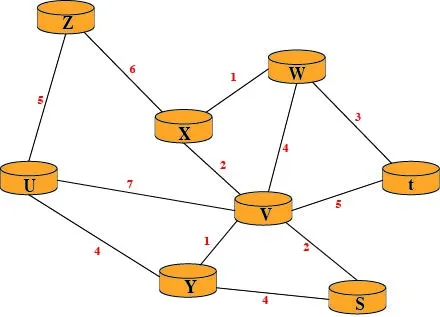
**2.3 Analyze the trade-offs between scalability, performance, and policy control in routing protocols.**

The Intra-AS is limited on the scalability and OSPF takes use of areas to scale. It is best used for speed and connection. The policy control is limited and takes use of costs and the metrics. There is also a smaller administrative overhead. The convergence time is recorded as very fast for OSPF and IS-IS and very slow for RIP. The uses of resources are more in LS protocols. Inter-AS has the ability to be highly scalability. It also has a very slow purposeful meeting. The policy control can be changed easily and changed for each router.

**Problem 3:**

Consider the network shown in the figure. With the indicated link costs, use Dijkstra’s shortest-path algorithm to compute the least-cost (shortest) path.

Show your work using a table similar to Table 5.1 (or the table on slide 17, page 12), do the following



* 1. **Compute the least-cost path from t to all network nodes.**

|  |  |  |
| --- | --- | --- |
| Destination | Cost | Path |
| T | 0 | T |
| W | 3 | T->W |
| X | 4 | T->W->X |
| V | 5 | T->V |
| Y | 6 | T->V->Y |
| S | 7 | T->V->S |
| Z | 10 | T->W->X->Z |
| U | 10 | T->V->Y->U |

* 1. **Compute the least-cost path from x to all network nodes.**

|  |  |  |
| --- | --- | --- |
| Destination | Cost | Path |
| X | 0 | X |
| W | 1 | X->W |
| V | 2 | X->V |
| Y | 3 | X->V->Y |
| T | 4 | X->W->T |
| S | 4 | X->V->S |
| Z | 6 | X->Z |
| U | 7 | X->V->Y->U |

**YouTube Videos**

Problem 1: <https://youtu.be/LZmKfsQcszM>

Problem 2: <https://youtu.be/mpB0N8HTT7s>

Problem 3: <https://youtu.be/Vj__bivegcE>