An Evaluative Analysis of DUAL, SPF, and Bellman-Ford

Shahab Tayeb* and Shahram Latifi

Department of Electrical & Computer Engineering, University of Nevada, Las Vegas, NV, United States
**Corresponding Author: shahab.tayeb@unlv.edu*

Received 17 October 2016; Accepted 27 November 2016;
Publication 10 December 2016

Abstract

This paper aims to discuss a comprehensive list of demerits associated with the use of Diffusing Update Algorithm compared to its link-state counterpart, namely, Shortest Path First algorithm which is a variant of Dijkstra's algorithm. Such a comparison was neglected for the past two decades due to the proprietary nature of the former protocol. This has led to the prevalence of the latter which is why many computer network professionals adamantly recommend implementing link-state protocols in campus implementations. However, this is of importance today pursuant to the release of several IETF Internet drafts in an attempt to standardize the Enhanced Interior Gateway Routing Protocol. Additionally, the results are compared with Bellman-Ford as a simple but widespread routing solution.

Dynamic routing protocols rely on algorithms computing the shortest paths using weighted digraphs and tree traversals. In this paper, not only are the algorithms discussed but also an in-depth analysis of the various features of the aforementioned protocols is conducted. Abandoning the periodicity of update massages and operating in an event-driven fashion with automatic failover capability are some of the features that will be analysed. Part of the novelty of this paper lies in the mathematical representation of decision-making processes and metric computation. One of the notable findings of this paper is an evaluative analysis of convergence times achieved in a typical university campus routing implementation. Moreover, using wide metric

Journal of Software Networking, 1–22.
doi: 10.13052/jsn2445-9739.2017.001

vectors contributes to energy-aware routing and improved performance for jitter-sensitive services.

Keywords: Convergence, Diffusing Update Algorithm, Routing Protocols, Shortest Path First Algorithm, Wide Metrics.

1 Introduction

In computer networks, packet forwarding and path selection decisions are based on information contained in routing information bases. Convergence of routing information bases depends on exchange of inter-router messages and updates by dynamic routing protocols and those protocols rely on algorithms computing the shortest paths using weighted digraphs, tree traversals, and finite state machines (FSM). Implementing dynamic routing, also called adaptive routing, is an integral part of any medium to enterprise-size computer network. Different protocols have been developed that can assist intermediary devices operating at or above network layer of the OSI model with learning about added, removed, or changed remote paths [1]. An alternative to routing protocols would be to manually configure fixed paths on each and every node using pre-computed paths which are installed as static routes in Routing Information Bases (RIB). These manual entries are limited to scenarios with fixed topology; however, they benefit from ease of implementation and configuration. They are less CPU and memory intensive and are considered more secure due to being unsusceptible against eavesdropping and spoofing attacks. Moreover, the paths taken by packets are predictable, which makes troubleshooting easier. However, such routes are only suitable for simple topologies as configuration complexity grows exponentially as the network scales. They are prone to configuration mistakes, lack scalability, and are incapable of reacting to network failures. Besides, any modification requires manual intervention. Static configurations are impractical in most real-world scenarios and production networks and are only used in special situations such as default routes [2].

Conversely, dynamic routing protocols are suitable for all topologies and their configuration complexity is generally independent of network sizes. They dynamically adapt to changes and failures. They are nevertheless more complex to implement and are generally considered less secure because of broadcast or multicast messages and updates. Selecting the most efficient dynamic routing protocols requires proper planning and is mainly a case by case analysis and varies by requirements and existing limitations like topology

depth. Moreover, knowledge of administrators is a conclusive factor. In this paper, we use a university campus network as our case study in this paper. One of the goals of this paper is to thoroughly highlight similarities and differences between link-state protocols and an FSM-based protocol such as Enhanced Interior Gateway Routing Protocol (EIGRP) [2].

Popularity of dynamic protocols changes over time. Web search popularity of widely-used protocols between January 2004 and April 2016 are illustrated in Figure 1. These numbers were obtained using Google search trends. A value of 100 is the peak popularity for the term. A value of 50 means that the term is half as popular. Likewise a score of 0 means the term was less than 1% as popular as the peak. It is noted that all routing protocols have lost their popularity significantly between 2004–2016 except EIGRP which only experienced a slight decline even though it has been a proprietary protocols and thus, not widely adopted. This holds great promise for the future of EIGRP as a standard.

The rest of this paper is organized as following: Section 2 summarizes an indispensable background for dynamic routing protocols. Section 3 is an exhaustive survey of EIGRP parameters and features, be it from the different versions of IETF Internet Draft or from EIGRP-specific configuration guides and white papers. Section 3 also presents the mathematical representations of metric computation and the decision making processes. Section 4 presents the experiment setup including the simulators and topology. Section 5 presents the simulation results. Section 6 discussed the wide-metric and the proposed science DMZ subnetwork as well as the circumscribed aspects of the case study and how they can be generalized to other implementations. Concluding remarks are given in Section 7.

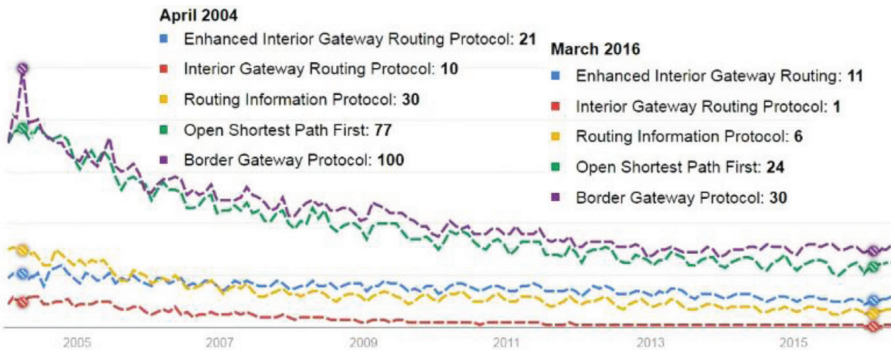

Figure 1 Popularity trends of dynamic routing protocols.

2 Background

2.1 Routing Information Base (RIB)

RIB, or routing table, is the data table stored on both intermediary and end devices operating at or above the network layer. It lists the routes to local, directly connected, or remote networks and includes reachability parameters such as metric, next hop address, and timers. In a fully converged network, packets are forwarded using the best paths without experiencing issues such as endless routing loops or suboptimal routing.

Virtual Routing and Forwarding (VRF) is a virtualization technique for co-existence of several RIBs on the same device, each of which are called instances. This enables using the same or overlapping IP addresses without conflict, as the instances are independent. VRF-Lite is the extension of VRF to customer-end equipment [3]. Another concept related to RIB is the topology network depth. This parameter is defined as the number of hops required for the information to reach all routers and/or layer 3 switches. Network depth can impact the convergence time.

2.2 Control Plane

Intermediary network devices and systems perform functions in three distinct areas of operation:

- Forwarding plane: This plane processes, mainly forward or filter, user-generated traffic. It is also known as data or user plane.
- Control plane: This plane connects to other intermediary devices and carries signalling traffic. Packets categorized in this layer are both generated by and destined to intermediary devices.
- Management plane: Using management plane, devices get their configuration and interact with the administrator.

Conventionally, these three planes are implemented in firmware, but frameworks like Software Defined Networking (SDN) decouple one or more of these layers from hardware and push them to software. Each of these ideally independent planes carries a different type of packet. Therefore, dynamic routing protocols are considered control plane. The milestone for the evolution of dynamic routing protocols is illustrated in Figure 2.

These protocols are divided into two categories of Exterior Gateway Protocols (EGP) and Interior Gateway Protocols (EGP), depending on whether they operate in a single Autonomous System (AS) or are capable of transferring routing information inter-AS. Border Gateway Protocol is the only protocol used to connect different organizations under different network

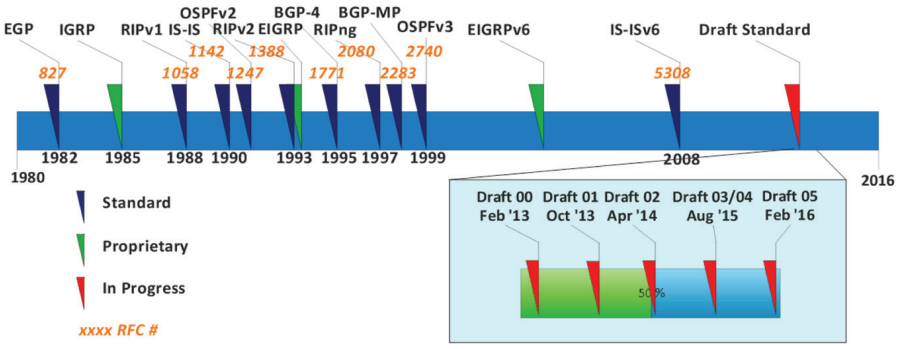

Figure 2 Evolution of dynamic routing protocols.

administration (different Autonomous Systems). No IP routing protocol is designed to do both with the exception of EIGRP. EIGRP is the only protocol capable of routing both inter-Autonomous System and intra-Autonomous System.

Switching and routing functionalities are converging into a single layer and there are many efforts to push as much computation as possible to the hardware, Application-Specific Integrated Circuit (ASIC) to be exact. Software trends also play a key role in proliferation of IP-based routing. Huang et al. [4] developed a web-based switching system, configured remotely using a Command Line Interface (CLI).

The aforementioned protocols handle unicast and broadcast communication in case for IPv4 and unicast for IPv6 but in order to route multicast or anycast, other protocols are required. Furthermore, content-based routing is an alternative routing protocol design [5, 6]. A generic SDN-based architecture for change management in routing is proposed in [7].

Network-on-chip (NoC) architectures have been prevalent in the past decade and there are efforts to enable NoC to route multicast traffic [8]. There have been many studies on the impact of IP layer and routing policies on multilayer network design [9]. Palkopoulou et al. [9] investigated different network planning and design approaches with varying hierarchical routing layers and suggest several key issues associated with such implementations.

3 EIGRP

EIGRP, formerly known as a Cisco-proprietary, is characterized as a distance vector routing protocol because of the inherent properties of Diffusing Update Algorithm (DUAL) such as rumour-based update packets from adjacent

neighbours. However, some features of EIGRP are those usually expected from link-state routing protocols like OSPF or IS-IS. Moreover, some properties of EIGRP even go beyond its link-state counterparts leading to faster convergence and improved resiliency. EIGRP benefits from the following features:

3.1 Diffusing Update ALgorithm (DUAL)

EIGRP computations are done by the DUAL FSM which is a workflow model composed of states, transitions, and operations. DUAL converges the control plane to a single set of loop free paths and backup routes throughout the routing domain [10, 11]. The loop free backup paths can be used immediately, leading to automatic failover that is transparent to end user. This loop-freedom at every instance is critical in ensuring network performance from the detrimental effects of routing loops. The next hop address for the path with the smallest weighted metric is denoted as Successor (*S**). From Reference [12], we can derive the operation of DUAL FSM as illustrated in Figure 3.

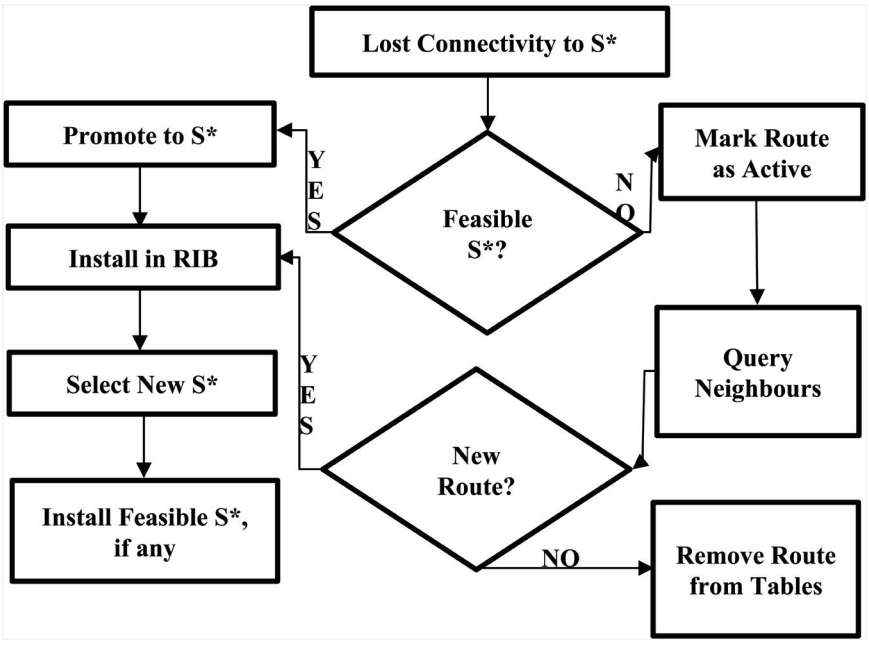

Figure 3 DUAL FSM.

3.2 Feasibility Condition (FC)

An integral part of DUAL and the main criterion used to make sure of loop-freedom in the computations is FC and is shown in the topology table. According to Reference [13], FC is "a sufficient but not a necessary condition"; i.e. every path meeting FC is guaranteed to be loop-free; however, not all loop-free paths meet FC. "The feasibility condition states that the reported distance of a route must be less than the feasible distance of the current successor route. In other words, in order to become a feasible successor, the reported distance of the feasible successor must be less than the feasible distance of the successor" [13].

Routes affected by a topology change should pass an FC check. They will either remain in "passive" state or need to enter an "active" state. The "active" state implies that the neighbour with the lowest metric meets FC whereas "passive" routes lack a neighbour meeting FC. Routes in "active" state are not installed in RIBs and thus, are not used to forward packets. In other words, when routers are actively seeking information, mainly about cost or next-hop address, about a specific remote network, those routes are marked as active in the topology table.

The path with the lowest calculated metric is denoted as the successor (S^*) whose metric is the sum of metric reported by the adjacent neighbour, Reported Distance (RD), and the metric from the local device to that neighbour, local distance (LD). This sum is called Feasible Distance of Successor (FD_S). From [13] we can derive the following Equation (1).

$$FD_S = RD + LD \tag{1}$$

An eligible backup is denoted as a Feasible Successor (FS). As explained above, this eligibility is determined by FC which states that in order to be considered as an *FS*, the *RD* must be less than or equal to FD_S as shown in Equation (2). For routes $i \in (0 \ldots r)$

$$RD_i \leq FD \tag{2}$$

More than one route may satisfy FC and if this is the case, DUAL can utilize them for unequal-cost load-balancing. This is done using a parameter called variance. Variance (V) is a multiplier that will be checked against Equation (3). For routes $i \in (0 \ldots r)$

$$FD_i \leq FD_S \times V \tag{3}$$

All route(s) satisfying Equation (3) can be installed in the routing table and used to forward traffic. By default, it is limited to 4 concurrent routes.

As a result of the default of $V = 1$, four routes with equal *FS* to FD_S will be installed as equal-cost load-balancing.

3.3 Packets

EIGRP uses several packet types to facilitate operational reliability and resiliency. These include: hello, query, reply, request, and update packets. Table 1 summarizes the properties of these packets based on [13]. These messages decouple establishing and maintaining of adjacencies from exchanging routing information. EIGRP messages are distinguished using a one-byte Opcode field in EIGRP packet header. These packets use 224.0.0.10 and FF02::A reserved multicast addresses for operation in IPv4 and IPv6 environments, respectively. If encapsulated in an Ethernet frame, 01-00-5E-00-00-0A is used as the destination MAC, physical, address in the header [13].

EIGRP-enabled devices establish adjacency with adjacent neighbours using periodic transmission of hello packets, at either five-second or sixty-second intervals by default. It should be noted that without symmetric configuration on adjacent neighbours, adjacency will be lost. The requirements for this symmetricity are: a) layer 3 connectivity between the two; b) no passive configuration; c) IP addresses in the same subnet; d) same authentication configuration; and e) K-values. Any mismatch results in route entries to

Table 1 Properties of EIGRP packets (sorted alphabetically)

Packet	Format	Description	OpCode	Reliability
Hello	Multicast Unicast[1,2]	Forms adjacency & agreement on parameters	5	Unreliable
Query	Multicast Unicast[3]	Transmitted when a route is "Active" state	3	Reliable
Reply	Unicast	Generated in response to Query packets	4	Reliable
Request	Multicast Unicast	Sent when specific information is required	2	Unreliable
Update	Multicast Unicast[4]	Conveys reachability information and initial warm-up	1	Reliable

1. Unicast: used for static adjacency.
2. Unicast: acknowledgement message.
3. Unicast: generated if no response to a multicast is received.
4. Unicast: transmitting a full table to a new neighbor.

be flushed from the tables and disastrous effects on network convergence. However, unlike OSPF, the following need not match: hello time, hold time, IP MTU, and router IDs [14].

Unlike its link-state counterparts, EIGRP is equipped with a goodbye message for faster convergence. A hello packet with all K-values set to 255 is generated to inform peers about the impending topology change. For improved reachability, it is generated as a broadcast packet. This feature is called graceful shutdown [15].

3.4 Transport

With a protocol type 88, EIGRP relies on its own Reliable Transport Protocol (RTP) operating at transport layer. RTP offers a balance of reliable and unreliable intermixed transmission of unicast and multicast packets, sending acknowledgement to packets that require it and sending replies in other cases. The use of RTP allows routers to initially exchange complete routing tables for initial synchronization followed by triggered, unbounded and partial updates afterwards. RTP is unique to EIGRP and sets the stage for DUAL via tracking the neighbor adjacencies and delivery and reception of EIGRP packets. Reliability is facilitated using acknowledgment messages which are empty hello packets and are always sent as unicast. As shown in Table 1, most EIGRP packets can be transmitted as either multicast or unicast depending on the scenario. The time to wait before switching from multicast to unicast is known as Multicast Flow Timer (MFT).

RTP utilizes two other timers: Retransmission TimeOut (RTO) and Smooth Round-Trip Time (SRTT). RTO is the time between transmission of subsequent unicasts and SRTT is the average elapsed time between transmission of EIGRP packets and reception of an acknowledgement. Both MFT and RTO are calculated based on SRTT, but the exact formula is proprietary. These parameters are found in adjacency tables.

3.5 Multivariate Metric

One of EIGRP's strengths lies in its complex multivariate metric that is based on several parameters. EIGRP initially used several metric components: bandwidth, delay, reliability, load, MTU, and hop count.

In order to signify the importance of each one of these components, six coefficients are introduced: $K_1,\ K_2 \ldots K_6$.

Let's denote bandwidth (B), delay (D), reliability (R), load (L), MTU, and hop count (H). Equation (4) can be inferred from [13] to compute the classic composite metric ($\hat{E}$) for a given route r.

$$\hat{E}_r = 256 \times \left[\left(\left\lfloor {}^{(K_1 \cdot 10^7)}\!/_{\min(B)} \right\rfloor + \left\lfloor {}^{K_2 \cdot 10^7}\!/_{\min(B) \cdot 256 - \max(L)} \right\rfloor + K_3 \cdot {}^{\sum_1^r D}\!/_{10} \right) \cdot {}^{K_5}\!/_{(K_4 + \min(R))} \right] \tag{4}$$

where *B* is expressed in Kpbs. Because of the reference value being 107, $\hat{E}$ supports *B* in the range of 1 Kbps and 10 Gbps. *D* estimates interface's serialization delay, expressed in tens of ms. *D* is used to poison an unreachable route by advertising it equal to 167,772,140, also called the infinite value. *R* and *L* are both expressed as a fraction of 255. *L* has a pair of counters: Tx_{load} and Rx_{load}. MTU and *H* do not impact Equation (4).

To calculate the composite metric with wide metrics where A is the extended metric and *T* is the throughput defined as:

$$T = \left({}^{RB \cdot WS}\!/_{B} \right)$$

Equation (5) shows the classic composite metric ($\ddot{E}$) for route *r*.

$$\ddot{E}_r = \left[\left(K_1 \cdot T + \left\{ {}^{K_2 \cdot T}\!/_{256 - \max(L)} \right\} + K_3 \cdot {}^{\sum_1^r D}\!/_{10} + K_6 \cdot A \right) \right] \times {}^{K_5}\!/_{(K_4 + \min(R))} \tag{5}$$

The default values for Wide Scale (WS) and Referred Bandwidth (RB) are 65536 and 107, respectively.

3.6 Authentication

Both Message-Digest 5 (MD5) and Secure Hash Algorithm-based (SHA-2) authentications are supported. This feature blocks spoofing attacks in an attempt to poison RIBs. Be that as it may, authentication does not encrypt the packets and hence, makes EIGRP prone to man-in-the-middle and eavesdropping attacks which can be mitigated using additional configuration and relying on other protocol encapsulations. Enabling authentication on EIGRP-enabled devices requires three steps:

i. Creating a keychain and one or more keys.
ii. Configuring EIGRP for either MD5 or SHA hashing mode.
iii. Configuring EIGRP to use that keychain and key [15–16].

The steps are identical on both IPv4 and IPv6 with the only difference that IPv6 is configured under interface mode, *Device-name(config-if)#*, rather than routing protocol global specific mode, represented as *Device-name(config-router)#*. This discrepancy is addressed in Named configuration mode [16].

3.7 Route Aggregation

EIGRP utilizes automatic aggregation as the default behaviour at the border of major networks/subnets. This behaviour can be useful for smaller plug-and-play scenarios as it simplifies the configuration for novice administrators, but should be disabled for larger implementations. Furthermore, EIGRP supports manual summarization, and if aligned with proper IP address planning, leads to scalability through shrinking update packets and RIB; therefore, aggregation takes the load off CPU and memory of the devices while utilizing less bandwidth.

Aggregation is performed using a multi-input XOR on IP subnets. The objective is to separate the left-most similar bits; hence, XOR is performed from the most significant bit until a non-similar bit is identified. All bits to the right of the non-similar bit are then changes to zero using AND operation.

3.8 Route Tags

EIRGP packets may contain a variable number of fields, each of which are tagged. This ensures easy integration of new capabilities and computability with older versions. This is demonstrated in packet header similarity between IPv4 and IPv6. Tagging and filtering internal and external routes can be implemented using distribute-lists, prefix-lists or route-maps This information is sent using Type/Length/Value (TLV) fields where a) Type is a binary code, usually represented alphanumerically, which defines the field category, b) Length is the value field shown in bytes, and c) Value is a series of bytes containing the data. TLV is a 32-bit triplet field.

3.9 Stub Feature

While passive interface configuration can stop all EIGRP packets by not establishing adjacencies on interface(s), stub feature can limit specific EIGRP packets while maintaining adjacencies. Stub routing offers such benefits in hub and spoke topologies as a) Improve network stability, b) Reduce memory and processor utilization, c) Reduce bandwidth utilization, and d) Simplified configuration [16]. There are several configurable stub options which makes

this feature flexible in various implementations: receive-only, connected, static, summary, and redistribute.

4 Experiments

The campus network studied in this paper is comprised of dozens of access layer devices which support over 16,000 wired workstations and 5,000 wireless end devices. These access layer equipment include Ethernet switches and Wireless Access Points which are connected to several intermediary devices at a collapsed core. Currently, there is no dedicated core device to support high bandwidth, low latency services.

4.1 Simulators

Computer assisted simulation are used in this study to model and analyse EIGRP behaviour based on the network model presented in Figure 4. Four different network simulators and emulators were utilized:

- Packet Tracer (PT) is a network simulation tool designed for Cisco Networking Academy courses. It was used because of its inherent support for most EIGRP commands and features [17].
- Wireshark, formerly known as Ethereal, is an open packet sniffer and analyser which uses Packet Capture (Pcap) for capturing streaming network traffic in real time. It was employed to capture and analyse control plane packets originated and destined to routers and layer 3 catalyst switches [18].
- Riverbed Modeller (RM), formerly known as OPNET, is a mature commercial network simulator, capable of modelling all network types and technologies. It is a simulator built on top of Discrete Event System (DES). In this study, it was used as a scalable solution to design and demonstrate communication networks [19].
- GNS3 network emulator was used to run and test EIGRP on actual Cisco Internetwork Operating System IOS images because of the limited capabilities of simulators in terms of supporting the various advanced features of heterogeneous network protocols [20].

4.2 Network Topology

The logical topology used in this series of experiments is shown in Figure 4. This network model is a simplistic view of a campus network and is comprised of several major modules: a) access layer devices, b) collapsed core devices

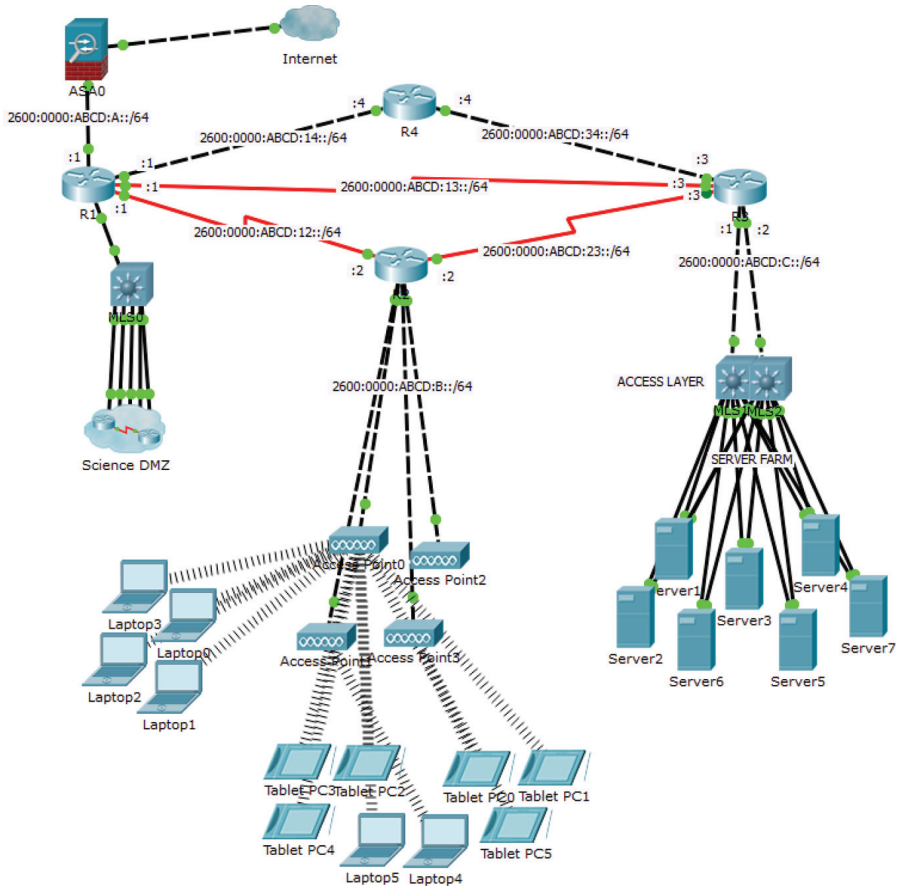

Figure 4 Logical topology of the experiment in packet tracer.

acting as both distribution and core layers, c) server farm, d) wireless ad-hoc networks and mesh wireless network, e) Adaptive Security Appliance (ASA) located in-line in the upward link towards external networks, particularly, the Internet, and f) a Science DMZ.

Several configurations were implemented on Figure 4: EIGRP for IPv4, OSPFv2, EIGRP for IPv6, and OSPFv3. The OS images used were C7200-ADVIPSERVICESK9, Ver. 15.2(4)S5 and C2900-UNIVERSALK9-M, Ver. 15.1(4)M4 used on 7200 and 2900 family series devices, respectively. Figure 5 illustrates the hierarchical topology of the experiment.

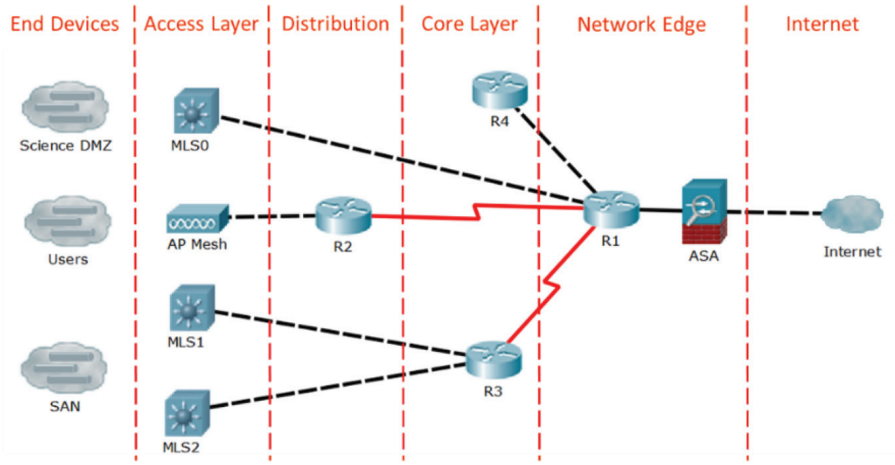

Figure 5 Hierarchical model of the experiment.

5 Results

The results of IPv4 simulations are presented in Figure 6a. A similar study was performed using IPv6; the results of which are presented in Figure 6b. To have a comprehensive comparative analysis of the aforementioned protocols, different parameters were measured. Cold start values represent the amount of time, in minutes, it took all devices for the initial convergence to populate their RIBs. Convergence time for addition of a new subnet is presented

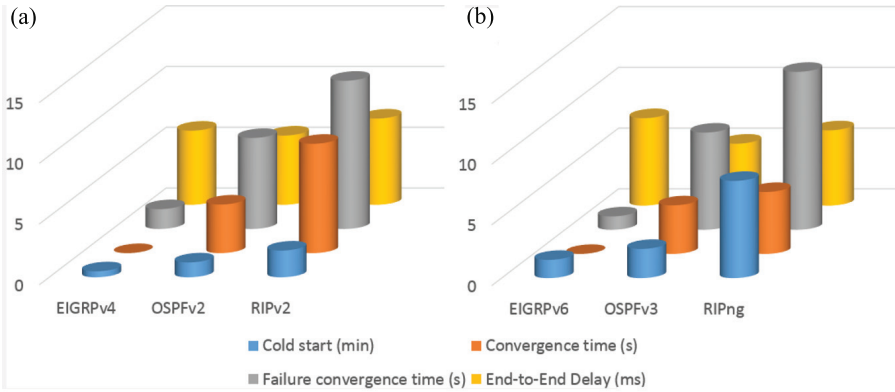

Figure 6 a) Comparative results between EIGRPv4, OSPFv2, and RIPv2; b) Comparative results between EIGRPv6, OSPFv3, and RIPng.

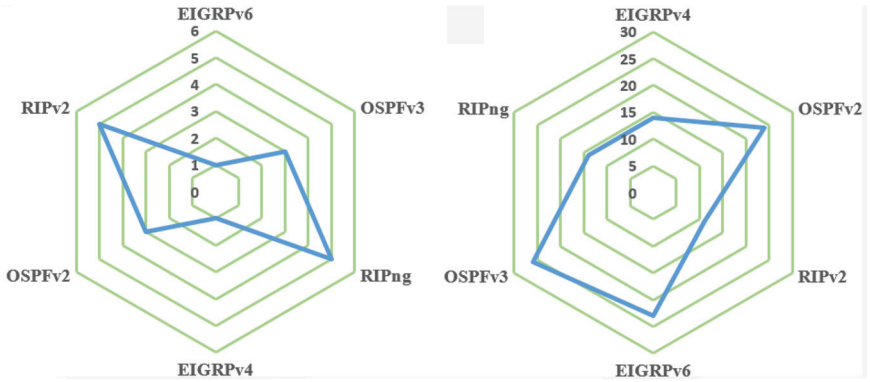

Figure 7 a) CPU usage in 1-min percentage; b) Packet loss in percentage.

as convergence time in seconds. A scheduled link failure and the resulted topology change are reflected in failure convergence time in seconds. End-to-end delay of the furthest device on the control plane, measured in milliseconds, is shown.

As it can be seen from Figure 7, EIGRP performs much better than its link-state counterpart in terms of cold start, convergence time, and in case of failure, at the expense of slightly more end-to-end delay. Finally, to demonstrate the load on device resources, 1-min CPU usage right after the peak of computations is also given in Figure 7a. The percentage of packet losses over the total number of packets is also shown in Figure 7b. EIGRPv4 demonstrated the lowest CPU usage among all the discussed protocols; however, expanding these findings to other devices and models needs further experiments. The main characteristics of EIGRP, OSPF, and RIP are outlined in Table 2.

6 Discussion

6.1 *K*-Values

K-values defined in Equation (6) can be interpreted as follows:

- K_1: This coefficient prioritizes decision based on throughput and relies on correct configuration of B values on serial interfaces and use of RB when dealing with high speed interfaces such as 10 Gbps or 100 Gbps. This value relies on initial setup by the administrator.

Table 2 Comparison of EIGRP and OSPF

	Routing Protocol		
Features	EIGRP	OSPFv2	RIPv2
Algorithm	DUAL	SPF	Bellman-ford
Hierarchy	Single-area, hierarchical using aggregation	Multi-area	Flat
Metric	Composite Equation (1) & Equation (2)	Cost (Bandwidth)	Hop count
IGP/EGP	Either IGP or EGP	Only IGP	Only IGP
Type	Distance Vector	Link State	Distance Vector
Aggregation	Automatic and Manual	Manual – limited to ABR/ASBR	Automatic and Manual
Complexity	Mediocre	Complicated	Simple
CPU	Low requirements	High requirements	Very low
Multiprotocol	IPv4/v6, IPX, and AppleTalk[1]	IPv4/v6	IPv4/v6
Standard	Formerly Cisco proprietary; currently an IETF Internet Draft	RFCs 1131, 1247, 1583, 2178, 2328, 2328	RFCs 1058, 1388, 1723, 2453, 4822
Load balancing	Equal/Unequal cost[2]	Only equal cost	Only equal cost

1. Supported using Protocol Dependent Modules (PDM).
2. Unequal: using variance as shown in Equation (3).

- K_2: This coefficient reflects congestion in the uplinks as a measure of L. These values do not rely on administrator intervention and can be utilized in flapping or unreliable connections.
- K_3: This multiplier highlights the use of D which is computed based on B. This makes it indirectly dependent on administrator configuration for K_1.
- K_4 and K_5: The impact of these multipliers is affected by noteworthy performance issues. This makes these two values effective when dealing with jitter-sensitive streaming services such as VoIP or videoconferencing. The threshold defined for tolerance of most streaming services is 1% packet loss [21].
- K_6: This coefficient was absent in earlier versions and reflects on the priority of aggregate metrics. As of the 4th version of the Internet Draft [13], extended attributes are accumulative jitter and energy [22].

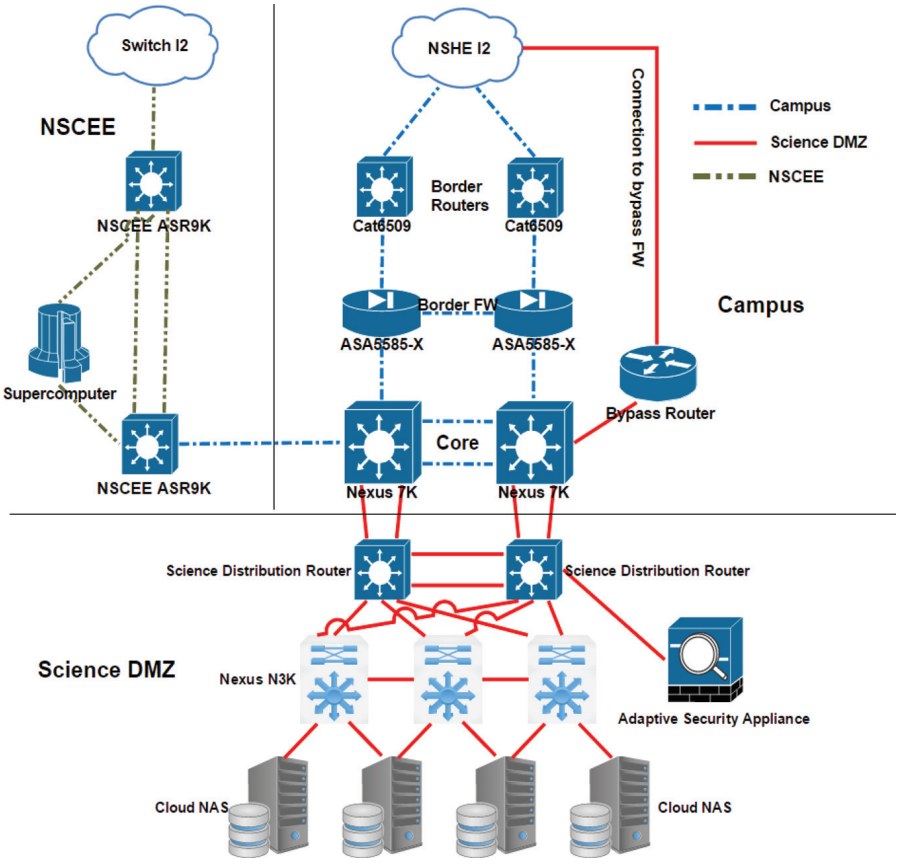

Figure 8 Logical topology of the proposed science DMZ topology.

6.2 Science DMZ

Figure 8 presents the proposed Science DMZ topology used as a proof-of-concept for scalability of the results to newer generations of educational networks.

6.3 Future Work

We hope our results will motivate more studies on DUAL as an underlying routing algorithm and EIGRP as a replacement for dominant network protocols in networks of different sizes. In particular, traffic engineering capabilities of EIGRP should be analysed. Additionally, applying EIGRP to other networks

such as Mobile Ad-Hoc networks (MANETs), Vehicular Ad-Hoc Networks (VANETs), and Wireless Sensor Networks (WSNs) will demonstrate usability for such applications. Compression of routing tables is also of interest in larger implementations of networks e.g., Internet backbone [23].

Only Cisco Internetwork Operating System could be used to run the simulations due to EIGRP still being a draft standard. The results of this simulation should be expanded to other network operating systems such as Juniper's Junos, Alcatel-Lucent's Service Router Operating System, Huawei's Versatile Routing Platform, or ZyXEL's ZyNOS. It should be noted that some advanced features of EIGRP, such as stub configuration, are missing from the current Internet Draft [13]. Stub configuration is required for Dynamic Multipoint Virtual Private Network (DMVPN) deployment.

7 Conclusion

We have proposed a replacement for one mature dynamic routing protocol with another newly standardized protocol, one that is proven as a proprietary protocol. Simulation and emulation results demonstrate that such a migration is justified. To facilitate this migration, performance of different aspects of the emerging standard were compared to its counterpart. These aspects included CPU usage, convergence time, packet loss, end-to-end delay, failure convergence time, and cold start. We concluded that EIGRP can provide shorter convergence times with minimal network traffic. This protocol used to be referred to as a hybrid; however, it is solely based on a distance vector algorithm and thus, should be referred to as advanced distance vector instead. Adding support for wide metric vectors, such as accumulative energy and jitter, using K6 which can be used for greener routing decision and improved performance for voice and video services. Similar to other distance vector protocols, Time-to-live (TTL) addresses the issue of count to infinity.

Acknowledgment

This work is supported in part by Doctoral Graduate Research Assistantship from UNLV Graduate College and in part by NSF award #EPS-IIA-1301726 (EPSCoR NEXUS). Authors also wish to acknowledge the valuable inputs provided by Mr. Robert Cray regarding the campus backbone architecture and connectivity.

References

[1] Malhotra. R. (2002). *IP Routing*. Sebastopol, CA: O'Reilly, 3–4.

[2] Routing protocols. (2014). *Companion Guide*. Indianapolis, Ind: Cisco Press, 161–163.

[3] Cisco. (2010). *Cisco Active Network. Abstraction Reference Guide*. San Jose, CA: Cisco Systems, Inc., 11–1.

[4] Huang, An-Cheng, Stig Thormodsrud, and Robert J., Pera. (2016). Network routing system. US. 15/048, 852.

[5] Jin, Y., Wen, Y., and Zhang, W. (2014). Content routing and lookup schemes using global bloom filter for content-delivery-as-a-service. *IEEE Syst. J*. 8, 268–278. doi: 10.1109/JSYST.2013.2253041

[6] Tao, M., Chen, E., Zhou, H., and Yu, W. (2016). "Content-centric sparse multicast beamforming for cache-enabled cloud RAN," in *Proceedings of the IEEE Transactions on Wireless Communications*, Rome, 15, 6118–6131. doi: 10.1109/TWC.2016.2578922

[7] Kohler, T., Dürr, F., and Rothermel, K. (2016). Consistent network management for software-defined networking based multicast. *IEEE Trans. Netw. Serv. Manag.* 13, 447–461. doi: 10.1109/TNSM.2016.2585672

[8] Duraisamy, K., Xue, Y., Bogdan, P., Pande, P. P. (2016). Multicast-aware high-performance wireless network-on-chip architectures. *IEEE Trans. Very Large Scale Integr. Syst*. 99, 1–14. doi: 10.1109/TVLSI.2016.2612647

[9] Palkopoulou, E., Gerstel, O., Stiakogiannakis, I., Telkamp, T., López, V., and Tomkoset, I. (2015). Impact of IP layer routing policy on multilayer design [invited]. *J. Opt. Commun. Netw*. 7.3: A396–A402.

[10] Garcia-Luna-Aceves, J. (1989). "A unified approach to loop-free routing using distance vectors or link states," in *Proceedings of the ACM SIGCOMM Computer Communication Review*, Vol. 19, Austin, TX, 212–223.

[11] Garcia-Lunes-Aceves, J. (1993). Loop-free routing using diffusing computations. *IEEE/ACM Trans. Netw*. 1, 130–141.

[12] Cisco Networking Academy (2014). *Scaling Networks Companion Guide*. Indianapolis, IN: Cisco Press.

[13] Savage, D. Ng, J., Moore, S., Slice, D., Paluch, P., and White, R. (2016). *Enhanced Interior Gateway Routing Protocol*. San Jose, CA: Cisco Systems Inc.

[14] Aziz, Z., Liu, J., Martey, A., and Faraz, S. (2002). *Troubleshooting IP Routing Protocols*. Indianapolis, Ind: Cisco Press.

[15] Cisco (2006). *Cisco IOS IP Configuration Guide*. San Jose, CA: Cisco Systems Inc.
[16] Cisco (2015). *IP Routing: EIGRP Configuration Guide*. San Jose, CA: Cisco Systems Inc.
[17] Packet Tracer (2009). *Cisco Networking Academy.* San Jose, CA: Cisco Systems Inc.
[18] Orebaugh, G. R., and Burke., J. (2007). *Wireshark & Ethereal Network Protocol Analyzer Toolkit*. Rockland, MA: Syngress Publishing.
[19] Chang, X. (1999). "Network simulations with OPNET," in *Proceedings of the Simulation Conference: Winter, Vol. 1* (Rome: IEEE), 307–314, doi: 10.1109/WSC.1999.823089
[20] Neumann, J. (2015). *The Book of GNS3*. San Francisco, CA: No Starch Press.
[21] Empson, S. (2013). *CCNA Routing and Switching Portable Command Guide: Enhanced Interior Gateway Routing Protocol (EIGRP)*, 3rd Edn. Indianapolis, IN: Cisco Press.
[22] Clark, A., and Claise, B. (2011). *Guidelines for Considering New Performance Metric Development*. Available at: http://www.rfc-editor.org/info/rfc6390 doi: 10.17487/RFC6390
[23] Karpilovsky, E., Caesar, M., Rexford, J., Shaikh, A., and van der Merwe, J. (2012). Practical Network-wide compression of IP routing tables. *IEEE Trans. Network Serv. Manag.* 9, 446–458. doi: 10.1109/TNSM.2012.081012.120246.

Biographies

S. Tayeb received the M.S. degree (Magna Cum Laude) in radio engineering and communications and the B.S. degree (Magna Cum Laude) in telecommunications engineering from the State Engineering University of Armenia in 2012 and 2010, respectively. He is currently a Ph.D. candidate in the department of electrical and computer engineering at University of

Nevada Las Vegas (UNLV). He holds CCIE R&S, CCDP, CCNP R&S, and CCAI from Cisco; CNSS 4011 Recognition from NSA; TKT from Cambridge; and VMCA-DCV from VMware. Prior to joining UNLV, he was an instructor and instructor trainer at Cisco Networking Academy where he was recognized as top %5 expert level instructors globally. He has been invited to deliver instructor-level courses in various countries around Europe, Middle East, Africa, and North America. He has authored/co-authored several research papers on network security, Wireless Sensors Networks, Internet of Things, and Big Data. His research interests span the areas of Internet of Things, Information Assurance, Security, and Wireless Sensor Networks utilizing such tools as Deep Learning and Big Data Analytics. He is a member of IEEE, ISOC, Teachers without Borders, and NSPE.

S. Latifi, an IEEE Fellow, received the Master of Science degree in Electrical Engineering from Fanni, Teheran University, Iran in 1980. He received the Master of Science and the Ph.D. degrees both in Electrical and Computer Engineering from Louisiana State University, Baton Rouge, in 1986 and 1989, respectively. He is currently a Professor of Electrical Engineering at the University of Nevada, Las Vegas. Dr. Latifi is the co-director of the Center for Information Technology and Algorithms (CITA) at UNLV. He has designed and taught undergraduate and graduate courses in the broad spectrum of Computer Science and Engineering in the past three decades. He has given seminars on cyber-related topics all over the world. He has authored over 250 technical articles in the areas of networking, cybersecurity, image processing, biosurveillance, biometrics, document analysis, fault tolerant computing, parallel processing, and data compression. His research has been funded by NSF, NASA, DOE, DoD, Boeing, Lockheed and Cray Inc. Dr. Latifi was an Associate Editor of the IEEE Transactions on Computers (1999–2006),

an IEEE Distinguished Speaker (1997–2000), and Co-founder and General Chair of the IEEE Int'l Conf. on Information Technology (2004–2015). Dr. Latifi is the recipient of several research awards, the most recent being the Silver State Research Award (2014). He is also a Registered Professional Engineer in the State of Nevada.