International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 7, No.3 (May-2018)

http://dx.doi.org/10.12785/ijcds/0703005

Data Security vs. Overall Performance in 6VPE

Sami Salih[1], AlAmeen Abdalrahman[1] and Kamal Elsharif [1]

[1]*College of Science and Art in Tabarjal, Al Jouf University, Saudi Arabia*

Received 13 Sep. 2017, Revised 04 Jan. 2018, Accepted 15 Feb. 2018, Published 01 May. 2018

Abstract: Both 6PE and 6VPE allow ISPs to provide end-to-end IPv6 connectivity over the legacy MPLS core networks. However, the security issues in IPv6 over Provider Edge Routers (6PE) lead to the development of IPv6 VPN Provider Edge Router (6VPE) with arguing that it's provide more secrecy to the IPv6 traffic in MPLS core. However, this method is yet to be evaluated in terms of performance and the level of secrecy. 6VPE adds the feature of creating VPN for each customer so that the private customer traffic is not disseminated among others. However, as MPLS uses labels to route traffic inside the ISP core network instead of the IP header; the overall network performance has to be confirmed. In this research a deductive methodology has been used to evaluate 6VPE configuration. Results shows an enhancement of 2.5% in the average round trip delay when using 6VPE compared to IPv4 traffic in MPLS.

Keywords: IP Address; MPLS; 6PE; 6VPE

1. INTRODUCTION

As the IPv6 has been deployed in the Internet core networks and many content providers provide service using the new protocol, various Internet Service Providers (ISPs) are lift behind due to the high cost of migration especially for MPLS core [1]. Therefore, the Internet Engineering Taskforce provides a solution to be utilized during the transition period which is 6PE. This method treats IPv6 as a label in MPLS routing and can achieve rapid deployment without any change in the core network [2]. However the pooling of all traffic in one broadcast domain raises major security concerns to the end customers. Hence, the development of separate VPNs for each end users in 6PE was proposed in the new RFC which known as 6VPE. The IETF published RFC 4798 [3] as a solution to be used during the transition period for MPLS core ISPs known as "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)" [3]. IPv6 traffic can be defined as a label in MPLS routing, its success to achieve rapid deployment without any change in the core network. However the pooling of all customer traffic in one broadcast domain raises major security concerns to the customers. Hence, the development of separate VPNs for each end user has been proposed in RFC 4659 [4] known as "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN". Creating such tunnels will eliminate any concerns regarding data privacy, however performance concerns has been raised in terms of stability, connectivity, and transmission security.

In this paper an MPLS test-bed has been implemented to provide end-to-end IPv6 connectivity using 6VPE. Then the overall performance regarding connectivity and data privacy has been evaluated.

The paper is structured as follows: IPv6 transition and its challenges has been discussed in Part two. Then, part three, presents 6VPE features and describes its operation method. Implementation scenario and discuss the findings and results are described and discussed in part four. Finally, part five drawns the conclusions.

2. TRANSITION TO IPV6

A. The need to a new protocol

The Internet continues to grow day-by-day, increased number of new users and applications are added to the network continuously. This leads to the fact that the current version of IP address (IPv4) space faces difficulties to satisfy the potential market demands. Actually, the available addresses from IPv4 were exhausted at the Internet Assigned Numbers Authority (IANA) level since February 2011 [2]. In 1998, the Internet Engineering Task Force (IETF) releases RFC 2460 which known as Internet Protocol, Version 6 (IPv6)". In this version, the address space exceeds to 3.4×10^38 unique address comparing to only 4.2×10^9 unique address in IPv4 [5]. The address exhaustion is the main reason for the transition. Moreover, designers of the new version benefit from the +40 years of experience in using IP, keeping all its strengths while

E-mail: shomer@ju.edu.sa, ameeneltoum@gmail.com, kamaleddin67@yahoo.com

adding new features such as auto-configuration, embedded multicast and the possibility to use end-to-end build-in security mechanisms which improves the Internet services.

B. Transition Mechanisms

An important aspect is that IPv4 and IPv6 are neither forward compatible nor backward compatible. This is due to the first field in the IP header which specifying the protocol version then the network node will act accordingly [5]. So the interoperability between them is not an option. Furthermore, we can't switch off the Internet to perform the migration overnight. Therefore, we need to define a period for the two versions to coexist using one of the coexistence techniques, namely dual-stacking, tunneling, and protocol translation [6], [7].

C. IPv6 Provider Edge Routers

In order to provide a communication channels to IPv6 customer in different geographic location is by setup tunnels via the dominant MPLS carriers. 6PE provides these channels to be setup automatically. The IPv6 customer should use a mapped IPv6 addresses to routes its traffic in the MPLS network [3].

The generic definition of a 6PE is a dual-stack IPv4 and IPv6-enabled router, with at least an IPv4 legitimate and routed address in the MPLS cloud and identified as a Forwarding Equivalence Class (FEC) with a correspondingly allocated and distributed label binding to the rest of the network.6PE is typically deployed by ISPs that have MPLS core network and (possible) supports MPLS VPN (or other) services [8] [9].

6PE uses two labels:

- The top label is the transport label, which is assigned hop−by−hop by the Label Distribution Protocol (LDP) or by MPLS traffic engineering (TE).
- The bottom label is the label assigned by the Border Gateway Protocol (BGP) and advertised by the internal BGP (iBGP) between the Provider Edge (PE) routers.

When the 6PE was released, a main requirement was that none of the MPLS core routers (the P routers) had to be IPv6−aware. That requirement drove the need for two labels in the data plane [10].

However, 6PE has a main drawback is which that it is have a single routing table. So, across the core all customer traffic are passing via the same pool. Thus customers traffic are not separated from each other as with Layer 3 MPLS-based VPNs. Hence for commodity Internet 6PE is a fair setup, and the customers need to protect their premises. However, if a site-to-site connectivity is required, a more privacy to be granted for each customer. In some cases its might also worth to consider using encryption between sites as an extra measure of security [11].

3. IPv6 VPN over Provider Edge Routers

The development of separate VPNs for each end user has been proposed in RFC 4659 known as "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN". Creating such tunnels will eliminate any concerns regarding data privacy, however performance concerns has been raised in terms of stability, connectivity, and transmission security [4].

Generally, in MPLS networks, VPN setup remains the same for IPv4 and IPv6 service. So, by just perform dual-stack configuration to the Provider Edge Routers (PE) IPv6 traffic can route without any other configuration in the MPLS core. Hence the 6VPE provides the same features as in IPv4 MPLS VPN [12].

6VPE router exchanges either IPv4 or IPv6 routing information through any of the supported routing protocols, and switches IPv4 and IPv6 traffic using the respective fast switching CEF or distributed CEF path over the native IPv4 and IPv6 VRF interfaces.

In 6VPE, the PE router disseminates routing information via Multiprotocol BGP. Thus, the same table is to be used to reaches other P and PE routers inside MPLS. However, different routing tables are preserved for dual-stacking [13] [14].

6VPE allows ISPs to offer IPv6 within VRFs, and is configured in the vpnv6 address family. It's logically the same as vpnv4, except that IPv6 addresses are exchanged between vpnv6 peers, not IPv4 addresses. Send-label is needed for 6PE, as that's how the PE routers coordinate their label assignments. Send-community extended is needed for 6vPE, as that's how the PE routers coordinate their RD/VRF/RT assignments. 6VPE enables to carry IPv6 global routes over an MPLS cloud, using vpnv6 BGP address family between the PEs [15] [16].

6VPE is a mechanism to use the IPv4 backbone to provide VPN IPv6 services. It takes advantage of operational IPv4 MPLS backbones, eliminating the need for dual-stacking within the MPLS core. This translates to savings in operational costs and addresses the security limitations of the 6PE approach. 6VPE is more like a regularIPv4 MPLS-VPN provider edge, with an addition of IPv6 support within VRF. It provides logically separate routing table entries for VPN member devices [14].

Also there are various approaches to control the security of a core if the VPN customer cannot or does not want to trust the service provider. IPsec from customer-controlled devices is one of them [16].

4. Implementation and Results

A. Simulation Environment

GNS3 is used to emulate an ISP scenario which provides end-to-end IPv6 connectivity to end users branches via IPv4 MPLS core. The following devices and tools are configured:

1) Cisco 7200 IOS: used for P (Provider Core Routers), PE (Providers Edge Routers), and CE (Customer Edge Routers).

2) Wireshark: is the capturing tool used to gather and analyze network traffic.

3) layer-2 switches: used as end-users LAN.

B. Network Topology

Fig. 1 shows the network topology consists of two core routers (P1 and P2), two Provider Edge routers (PE1 and PE2), and four Customer Edge routers for customer A and B (CEA1, CEA2, CEB1, and CEB2).

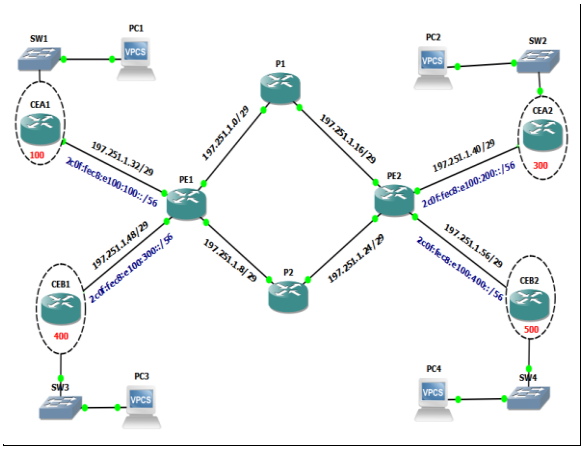

Figure 1. Simple ISP Topology

C. Network Address Configuration

1) CE Routers

TABLE I. CE ROUTERS CONFIGURATION

CEA1		
LAN Interface	IPv4	197.251.1.65/29
	IPv6	2c0f:fec8:e100:500::1/56
WAN Interface	IPv4	197.251.1.34/29
	IPv6	2c0f:fec8:e100:100::2/56
CEA2		
LAN Interface	IPv4	197.251.1.73/29
	IPv6	2c0f:fec8:e100:600::1/56
WAN Interface	IPv4	197.251.1.42/29
	IPv6	2c0f:fec8:e100:200::2/56
CEB1		
LAN Interface	IPv4	197.251.1.81/29
	IPv6	2c0f:fec8:e100:700::1/56
WAN Interface	IPv4	197.251.1.50/29
	IPv6	2c0f:fec8:e100:300::2/56
CEB2		
LAN Interface	IPv4	197.251.1.89/29
	IPv6	2c0f:fec8:e100:800::1/56
WAN Interface	IPv4	197.251.1.58/29
	IPv6	2c0f:fec8:e100:400::2/56

2) Provide (P) router

TABLE II. P ROUTERS CONFIGURATION

P1	
G-Eth 0/0	197.251.1.2/29
G-Eth 1/0	197.251.1.18/29
P2	
G-Eth 0/0	197.251.1.10/29
G-Eth 1/0	197.251.1.26/29

3) Provide edge (PE) router

TABLE III. PE ROUTERS CONFIGURATION

PE1		
G-Eth 0/0	IPv4	197.251.1.1/29
G-Eth 1/0	IPv4	197.251.1.9/29
G-Eth 2/0	IPv4	197.251.1.33/29
	IPv6	2c0f:fec8:e100:100::1/56
G-Eth 3/0	IPv4	197.251.1.49/29
	IPv6	2c0f:fec8:e100:300::2/56
PE1		
G-Eth 0/0	IPv4	197.251.1.17/29
G-Eth 1/0	IPv4	197.251.1.25/29
G-Eth 2/0	IPv4	197.251.1.41/29
	IPv6	2c0f:fec8:e100:200::1/56
G-Eth 3/0	IPv4	197.251.1.57/29
	IPv6	2c0f:fec8:e100:400::2/56

D. Network Configuration

1) IPv4 Connectivity: The following configuration is necessary to setup end-to-end IPv4 connectivity between the CE routers:

- OSPF is configured in the MPLS core network. Fig. 2 shows the verification of the OSPF neighbor.
- VRFs have been created and associated with the customer interfaces a router distinguisher (RD) to separate customer's route from each other [13]. Fig. 3 shows the MPLS verification.
- MP-BGP is configured in PE routers to advertise VRFs routes. Fig. 4 show the VRF tables.
- OSPF is configured between CE and PE routers to advertise customer site's routes to PE routers. Fig. 5 shows OSPF configuration.

```
PE1#sh ip ospf 1 neighbor

Neighbor  ID   Pri   State      Dead Time   Addresss      Interface
41.67.0.8       1   FULL/BDR   00:00:33    197.251.1.10  GigabitEthernet2/0
41.67.0.7       1   FULL/BDR   00:00:34    197.251.1.2   GigabitEthernet1/0
```

Figure 2. OSPF Neighbor

```
PE1#sh mpls interfaces
Interface              IP            Tunnel   BGP    Static  Operational
GigabitEthernet1/0     Yes (ldp)     No       No     No      Yes
GigabitEthernet2/0     Yes (ldp)     No       No     No      Yes
```

Figure 3. MPLS Verification

```
PE1#sh vrf brief
  Name                             Default RD          Protocols   Interface
  CEA1                             200:1               ipv4, ipv6  Gi3/0
  CEA1                             200:2               ipv4, ipv6  Gi4/0
```

Figure 4. VRFs Table

```
router ospf 2 vrf CEA1
 log-adjacency-changes
 redistribute bgp 200 subnets
 network 197.251.1.33 0.0.0.0 area 0
!
router ospf 3 vrf CEB1
 log-adjacency-changes
 redistribute bgp 200 subnets
 network 197.251.1.49 0.0.0.0 area 0
!
```

Figure 5. CE-PE OSPF routing

2) 6VPE Configuring: To setup an end-to-end IPv6 (6VPE) connectivity between CE routers, a BGP session is required between PE-CE routers. Loopback address is configured with IPv4 address in CE routers to ensure the BGP process gets the router Id to establish session with PE routers. VRFs address family separates IPv6 customer site's route from the other site. Similar configurations applied to (PE1-CEB1), (PE2-CEA2), and (PE2-CEB2) to brought up the BGP IPv6 unicast peering. Fig. 6 shows the verification of the VPNv6 setup.

```
PE1#SH bgp vpnv6 unicast all summary
BGP router identifier 41.67.0.5, local AS number 200
BGP table version is 13, main routing table version 13
8 network entries using 1344 bytes of memory
10 path entries using 800 bytes of memory
8/6 BGP path/bestpath attribute entries using 1056 bytes of memory
4 BGP AS-PATH entries using 96 bytes of memory
6 BGP extended community entries using 208 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 3504 total bytes of memory
BGP activity 20/0 prefixes, 22/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
41.67.0.6       4          200     140     142       13    0    0 01:56:34        4
2C0F:FEC8:E100:100::2
                4          100     133     133       13    0    0 01:57:24        2
2C0F:FEC8:E100:300::2
                4          400     132     133       13    0    0 01:57:20        2
```

Figure 6. VPNv6 Verification

3) IPSEC Configuration: IPsec has been configured in CE routers. Its provides two options of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well. IPsec can be run in either transport mode or tunnel mode. Transport mode is the default mode for IPsec, and it is used for end-to-end communications and IPsec tunnel mode is useful for protecting traffic between different networks, when traffic must pass through an intermediate, untrusted network. For this's reason IPSEC tunnel modes will be configured in CE routers to protect traffic of customer's site [15]. Fig. 7 and Fig. 8 show the Crypto ISAKMP SA for IPv4 and IPv6 traffic respectivly.

```
CEA1#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id  status
197.251.1.42    197.251.1.34    QM_IDLE           1002  ACTIVE
```

Figure 7. IPv4 Crypto ISAKMP SA

```
IPv6 Crypto ISAKMP SA
dst:    2C0F:FEC8:E100:100::2
src:    2C0F:FEC8:E1100:200::2
state:  QM_IDLE          conn-id:  1001    status: ACTIVE
```

Figure 8. IPv6 Crypto ISAKMP SA

E. Results and discussion

This section shows the relevant screenshots to prove the functionality of the test-bed and its configuration as well as the performance measurements of the overall network.

1) End-to-End Connectivity: Fig. 9 and Fig. 10 shows the end-to-end connectivity for both IPv4 and IPv6 traffic respectivily.

```
PC1> ping 197.251.1.74
84 bytes from 197.251.1.74 icmp_sec=1 ttl=62 time=828.048 ms
84 bytes from 197.251.1.74 icmp_sec=2 ttl=62 time=856.049 ms
84 bytes from 197.251.1.74 icmp_sec=3 ttl=62 time=841.048 ms
84 bytes from 197.251.1.74 icmp_sec=4 ttl=62 time=853.049 ms
84 bytes from 197.251.1.74 icmp_sec=5 ttl=62 time=778.044 ms
```

Figure 9. End-to-End connectivity for IPv4

```
PC1> ping 2c0f:fec8:e100:600::2

2c0f:fec8:e100:600::2 icmp_sec=1 ttl=60 time=917.052 ms
2c0f:fec8:e100:600::2 icmp_sec=1 ttl=60 time=746.043 ms
2c0f:fec8:e100:600::2 icmp_sec=1 ttl=60 time=761.043 ms
2c0f:fec8:e100:600::2 icmp_sec=1 ttl=60 time=813.047 ms
2c0f:fec8:e100:600::2 icmp_sec=1 ttl=60 time=819.047 ms
```

Figure 10. End-to-End connectivity for IPv6

2) Traffic Route: As Fig. 11 shows, the CE router forwards packet to PE router and because of the fact that CE router is not aware about what is the technology used inside the core, so CE router can't recognize how the packets forward between P routers. Also as showing PE router inject two labels (17/24) before forwards packet to P routers, one of them is normal label which P router use to forward packets and other one is VPN label which PE routers use in VPN process and P routers.

```
CEA1#traceroute 2c0f:fec8:e100:200::2
Type escape sequence to abort.
Tracing the route to 2C0F:FEC8:E100:200::2
  1  2C0F:FEC8:E100:100::2  172 msec  100 msec  188 msec
  2  ::ffff:197.251.1.10 [MPLS: Labels 17/24 Exp 0] 732  msec  536  msec  652  msec
  3  2C0F:FEC8:E100::1 [AS 200] 744 msec 588 msec 608 msec
  4  2C0F:FEC8:E100::2 [AS 200] 768 msec 592 msec 816 msec
```

Figure 11. Trace route between CE routers

3) Round trip delay: Fig. 9 and Fig. 10 shows the end-to-end round trip time from ECA1 to CEA2 using both IPv4 and IPv6 respectively. The average difference in round trip delay between native IPv4 and IPv6 tunnel is about 2.5%. Interestingly, the average percentage is shows IPv6 traffic performs better than its carrier IPv4. This due to the very short tunnel path with one trip compared to two trips from the source and two trips toward destination.

4) Overall performance: 6VPE is used to provide VPN IPV6 service in IPv4 MPLS core. It is considered one of the best solution as it takes the advantages of operational MPLS IPV4 infrastructure and also provides many benefits to service provider:

- IPv6 Transport with minimal operation cost and risk– While the service providers slowly move their infrastructure to support IPv6, they can use their existing IPv4 MPLS infrastructure to support IPv6.
- Provider Edge routers upgrade only.
- No impact on IPv6 customer edge routers.
- Privacy: Routers maintain separate routing tables for each VPN that they are connected to, called Virtual Routing and Forwarding tables (VRFs) Any IP packets that enter the MPLS L3VPN backbone network must enter on either a physical or logical interface that is defined to be within a specific VRF. Once a packet enters on an ingress VRF interface, it can only exit out an egress interface that is in the same VRF. This ensures that traffic is isolated between different VRFs.
- IPSEC is used with 6VPE to provide Encryption in case that customer s don't trust service provide and MPLS does not imply any type of encryption so customer can encrypt their traffic using IPSEC in CE router.

5. CONCLUSION

The security issues of 6PE has been discussed as the main point in this research. Moreover, the a 6VPE test environemnt has been implemented to structure an IPV6 VPN service in IPv4 only MPLS provider. As a result, information security improved due to the separate tunnels established for each customer.

Furthermore, from the overall performance test verify that no considrable decreases has been notices when IPv6 traffic uses 6VPE. Instead, the ISP system throughput should gain a significant improvement when native IPv6 is applied.

REFERENCES

[1] google, ipv6 statistics

[2] Sami Salih, Jordi Palet Martínez, Latif Ladid, Sureswaran Ramadass, “Guidelines to the Implementation of National Integrated Strategic Plan to IPv6 Transition”, International Journal of Scientific & Engineering Research, Volume 7, Issue 11, November-2016, ISSN 2229-5518

[3] J. De Clercq, D. Ooms, S. Prevost, F. Le Faucheur, “Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)”, IETF, DOI: 10.17487/RFC4798, February 2007.

[4] J, De Clercq, D. Ooms, M. Carugi, F. Le Faucheur, “BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN”, IETF, Multiprotocol Label Switching Architecture

[5] S. Deering, R. Hinden, “Internet Protocol, Version 6 (IPv6)”, Specification, IETF RFC 2460, 1998.

[6] I. Raicu; S. Zeadally, “Evaluating IPv4 to IPv6 transition mechanisms”, 10th International Conference on Telecommunications, 2003.

[7] Saadullah Kalwar; Nafeesa Bohra; Aftab A. Memon, “A survey of transition mechanisms from IPv4 to IPv6 — Simulated test bed and analysis”, 3rd International Conference on Digital Information, Networking, and Wireless Communications (DINWC), 2015.

[8] E. Rosen, A. Viswanathan, R. Callon, “Multiprotocol Label Switching Architecture”, IETF, DOI: 10.17487/RFC3031, January 2001.

[9] Cisco, multiprotocol-label-switching-mpls

[10] Parisa Grayeli, Shahram Sarkani, Thomas Mazzuchi, “Performance Analysis of IPv6 Transition Mechanisms over MPLS”, International Journal of Communication Networks and Information Security (IJCNIS) Vol. 4, No. 2, August 2012.

[11] Scott Hogg, & Eric Vyncke, “IPv6 over MPLS Security”, chapter 4 in “IPv6 Security”, Cisco Press, Dec 2008.

[12] E. Rosen, Y. Rekhter, “BGP/MPLS IP Virtual Private Networks (VPNs)”, IETF, DOI: 10.17487/RFC4364, February 2006.

[13] Wim Verrydt, Ciprian Popoviciu, “Study of IPv6 Multicast Deployment in MPLS Network”, International Multi-Conference on Computing in the Global Information Technology, ICCGI 2006.

[14] S. Kent, R. Atkinson, “Security Architecture for the Internet Protocol”, IETF DOI: 10.17487/RFC2401, 1998.

[15] Xin Wen, Changqiao Xu, Jianfeng Guan, “Performance investigation of IPSEC protocal over IPv6 network”, International Conference on Advanced Intelligence and Awarenss Internet, AIAI 2010.

Sami Salih, Assistant Professor in Al Jouf University. He found and yet chair the Sudanese IPv6 Task Force (SDv6TF), and he was the chair of the 2nd corresponding specialized group of IPv6 in the International Telecommunication Union (ITU). During his position at the telecom regulatory authority (NTC Sudan) as head of R&D he participated and contributed to the development of ICTs in his region, indeed he is appointed by ITU to develop a national migration plans toward deploying IPv6. Furthermore, he establish a specialized training center for IPv6 in Sudan in collaboration with USM NAV6 Malaysia. Currently as SudREN (Sudanese Research and Education Network) CEO, he conduct a project to provide e-services with IPv6 enable for all members institutes. On November 2014 Dr. Sami has been elected as AFRINIC PDWG Co-chair.

Alameen Eltoum Mohamed Abdalrahman, Assistant professor in Information Systems and computer Sciences at Aljouf University (KSA) and Alneealin University (Sudan). He has nine years of teaching and research experience. He is the head of computer science dapartment at colleage of Science and Art-Tabarjal.

Kamal El Din Mohamed El Sherif, he is a specialist in Information Security & Computer Networks with 12 year teaching experience in Al Jouf University - Saudi Arabia. His research interest including information network security, big data, and future network.