Afghanistan Research and Educational Network (AfgREN) Infrastructure

Assistant Prof. Mohammad Tariq Meeran
Information Technology Department
Computer Science Faculty, Kabul University
E-mail: tariqmeeran@ku.edu.af, tariqmeeran@yahoo.com

1 Abstract
AfgREN is a national research and educational network (NREN) for the Afghanistan’s academic community which was initially and unofficially formed in 2006. AfgREN focuses on supporting and providing high speed network backbone to universities, higher education institutions, teaching hospitals, libraries and research centers at national level. This will allow the academia to have access to the Internet, online resources, digital libraries, international research communities, e-communication, distance learning, e-learning, tele/video conferencing and knowledge sharing. AfgREN will also represent all higher education institutions to donor agencies, ISPs and other organizations. AfgREN will also include a Computer Emergency Response Team (AfgREN-CERT) to have coordinated response for the security threats. As a result all these services provisioning and support lead to a sustainable infrastructure for facilitating quality research and development efforts. In order to achieve these goals a very strong network infrastructure with a long-term technical and financial support is required. AfgREN’s goal is to plan, implement, operate, maintain and support such an infrastructure. Currently most of the major educational institutions are connected via Fiber Optic or Satellite links to the Internet in an unorganized manner from the perspective of a NREN, while the NRENs should be built in such a way that the educational institutions are connected with national high speed dedicated point to point links to each other and then from one central point to the Internet or international links. This paper discusses the current infrastructure, the proposed physical and logical infrastructure, proposed bandwidth, monitoring, security, management, sustainability and milestones.

2 Introduction
The National Research and Educational Networks (NRENs) are the driving force for every country's academic needs, research, development, e-learning, distance education, online resources, digital libraries, online research papers, tele/video conferencing and e-communication. Afghanistan’s academic community requires such an infrastructure that can provide the above mentioned services, in order to support the higher educational system and contribute in the countries development process and be an active member of the international educational community.

Considering the need for an NREN the NATO Public Diplomacy Division along with the Kabul University Lecturers initiated the process of building an NREN in 2006. This NREN was unofficially named Afghanistan’s Research and Educational Network (AfgREN). These efforts started with installing a Satellite link at Information Technology Center of Kabul University for the provision of Internet services. Sooner the NATO started to support various other infrastructural projects using their Network Infrastructure Grants.
(NIGs). Using these NIGs a Campus Fiber Optic Network was completed in mid 2007 for Kabul University which also included connectivity to the Ministry of Higher Education, boys and girls hostels. And meanwhile several other NIGs were provided to extend the Internet services from Kabul University to other Kabul–based Universities. These efforts continued in provision of Internet links and Campus Fiber Optic networks for several other Universities and this process is still continuing.

NRENs in general are like special ISPs [4] that provide services on a shared and cost effective infrastructure to the educational institutions and special research and development projects [Wikipedia, The Free Encyclopedia. Retrieved 16:30, August 7, 2013, from http://en.wikipedia.org]. In Afghanistan forming such an ISP and collecting service fees from the governmental universities are not possible considering the current financial system procedures and the way the budgets are allocated and spent. Therefore the MoHE decided to consider AfgREN as one of its own key infrastructural projects and included this project in its strategic plan in 2011 and started to expand and support it [Strategic Plan of Ministry of Higher Education. Retrieved 14:00, November 6th, 2013 from http://mohe.gov.af/?p=plan].

In this paper the AfgREN current topology, which is built as a result of six years efforts will be discussed. Then we will propose an infrastructure for the transformation of current topology to a new and sustainable topology. The proposed physical topology, logical topology, monitoring and security requirements will also be part of this discussion. We will also discuss the bandwidth requirements, sustainability issues and milestones of the AfgREN Infrastructure and its survival.

3 Current Topology

Currently the way the universities are connected to each other is using the Internet links through Satellite and Fiber Optic technologies [1]. These links will only enable the universities to connect to the Internet, but in order for these universities to communicate with other national universities and the MoHE data center or any other national university’s data center services they will have to use the Internet links and their traffic travels outside the country and then comes back to the national universities. This method of communication is not good and suitable for the academic institutions and such type of national communication. Because first of all the direct links to the Internet is expensive and therefore the bandwidth will be limited. Besides the national traffic travels outside the country and gets routed through the ISPs’ routers and then travels back into the country, this will result in unnecessary delay, security issues, load on Internet links and poor quality of service. In the long-run this type of connectivity for a research and educational network isn’t suitable, affordable and effective.

The Universities and Higher Educational Institutions current physical topology is shown in the below diagram. These connections are mix of fiber optic connections and satellite links. The fiber optic connections are provided through AFTEL and the satellite links are provided by Vizada and Neda. The allocated bandwidth for each university is shown in Figure 1.
The current logical addressing plan is based on the service providers address space like Vizada, AfTEL and Neda. In other words AfgREN doesn’t own these addresses and will only be in use by the universities till the service providers’ contracts are valid; once the contracts are terminated these addresses will be taken back by the providers. This will cause service interruptions and difficulty in hosting public services and reconfiguration issues.

4 Proposed Infrastructure
Modern NRENs in today’s world are directly connected to each other using dedicated high speed point-to-point links. These dedicated links are provided using the national ISPs and TSPs capabilities and their service availability at various locations. The best type of connectivity for AfgREN is fiber optic connectivity using the national fiber optic backbone, where fiber optic connections are not available then other types of connectivity like microwave or satellite can be considered as an alternate solution.

In order for the AfgREN infrastructure to be effective from the type of services point of view, cost, quality of service, sustainability factors, it should use the national service providers’ backbone infrastructure. This type of connectivity will be affordable, faster and effective [2]. Besides it will increase the national service providers’ user base and it will make their backbone stronger and richer.
4.1 Physical Topology

The proposed AfgREN physical topology is including an AfgREN NOC located at Kabul University, Fiber Optic Gigabit Metro Ethernet or 155 Mbps (1xSTM 1) connections between the NOC and each Kabul-based university, one STM 1 link from the AfgREN NOC to each large provincial university, 51 Mbps (1xSTM 0) or 34 Mbps (E3) for each small university and each provincial university’s sub-campus. The STM links can be configured with Domestic Private Lease Circuit (DPLC) connection. Universities that are located in the areas where the fiber optic connections are not available, they can be connected either through microwave point to point links or through satellite links. Depending on the AfTELs fiber optic backbone layout and availability a number of small provincial universities can be connected to the large provincial universities using STM 0 or E3 links [A. S. Nasimzada-Afghan Telecom, Afghanistan Optical Fiber Network, e-mail communication, 21st August 2013]. Figure 2 shows the physical topology details; incase STM 0 links are not technologically available instead E3 links which can provide 34 Mbps can be considered.

![AfgREN Proposed Physical Infrastructure](image)

Based on the above topology a 4-phase implementation plan has been prepared. Phase 0 is focusing on providing fiber optic connectivity for the universities that are not yet physically connected to fiber optic links. Phase 1 includes the migration plan from the fiber optic Internet links to the fiber optic DPLC links for the Kabul-based universities. Phase 2 covers the migration plan for the provincial universities fiber optic
Internet links to the DPLC links. Phase 3 plans for migration of the provincial universities satellite Internet links either to fiber optic DPLC links or microwave point-to-point links depending on the availability of connection options at each site. Phase 0 and part of phase 1 has already started and some of the connections are completed and some are still in progress. Figure 3 shows the implementation phases summary.

Figure 3 AfgREN Implementation Phases

4.2 Logical Topology
The proposed logical topology of AfgREN can be engineered using the hierarchical design model [6]. This model will consist of a core layer at the AfgREN NOC, distribution layer at each university and an access layer at each university’s campus. This model also includes a network edge for the security implementation and a WAN and Internet edge for dedicated point-to-point links to other universities and International links (Internet). The IP addressing structure can also be planned considering this model where each university will have its own public IP subnet while these subnets could be further subnetted for each universities internal use [5]. At each university’s distribution layer route summarization and security solutions can be configured to increase the routing performance and protect the campus networks from network security threats. At the core layer the route summarization can be used again to represent and advertise AfgREN as one supernet with a particular autonomous system number to the external networks. The Autonomous system number for AfgREN has already been issued by APNIC (Asia Pacific Network Information Center) which is (AS132467) and named: AFGREN-AS-AP. Figure 4 shows the proposed logical topology.
Addressing the AfgREN infrastructure can be done in several ways, the recommended practice is to have one registered public network address under AfgREN name and then subnet it based on the universities' requirements or size of the universities considering the route summarization and efficient routing best practices. Recently the University College London (UCL) agreed to provide a public network address that could be used by AfgREN on loan basis [Minutes of the 2nd AfgREN Technical Committee Meeting 1st December 2012], this address is 128.41.128.0/17 [P. Kristein, S. Varakliotis-University College London, Public IP address on long-term loan, e-mail communication August 18th, 2012]. This address is sufficient for the current structure and AfgREN’s proposed infrastructure for several years, since it can provide around 32000 public IP addresses, while the current number of addresses is around 4000, which is provided by Vizada Networks. Since there is also a plan to move towards using IPv6, and this may happen sooner according to the MCIT plan, this network address will be sufficient till the migration of AfgREN to IPv6. This address has been further subnetted based on the size of the universities. The size of the universities can be determined by the number of academic staff, employees and students. Table 1 shows the proposed address plan based on the size of universities, regardless of the current number of hosts on the existing
networks, since at the moment campus networks of most universities don’t exist and the universities are not fully equipped with computing equipments. For large universities a network address with a subnet mask of /20 is proposed, which provides 4094 addresses for each university and they can subnet it further to create logical divisions in their campus networks based on type of traffic, organizational structure or any other preference. For medium sized universities a network address with a subnet mask of /23 is considered which provides 510 addresses, and for small universities a network address with a subnet mask of /25 is considered, which provides 126 addresses. A few address blocks have been kept aside as a reserve for the future use and network expansion.

<table>
<thead>
<tr>
<th>Network Address</th>
<th>Subnet Mask</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>128.41.128.0</td>
<td>/20</td>
<td>Large University</td>
</tr>
<tr>
<td>128.41.144.0</td>
<td>/20</td>
<td>Large University</td>
</tr>
<tr>
<td>128.41.160.0</td>
<td>/20</td>
<td>Large University</td>
</tr>
<tr>
<td>128.41.176.0</td>
<td>/20</td>
<td>Large University</td>
</tr>
<tr>
<td>128.41.192.0</td>
<td>/20</td>
<td>Large University</td>
</tr>
<tr>
<td>128.41.208.0</td>
<td>/20</td>
<td>Large University</td>
</tr>
<tr>
<td>128.41.224.0</td>
<td>/20</td>
<td>Large University</td>
</tr>
<tr>
<td>128.41.240.0</td>
<td>/20</td>
<td>For Further Subnetting</td>
</tr>
<tr>
<td>128.41.240.0</td>
<td>/23</td>
<td>Medium Size Universities</td>
</tr>
<tr>
<td>128.41.240.0</td>
<td>/25</td>
<td>Small Universities</td>
</tr>
</tbody>
</table>

### Table 1 Public IP subnets and address allocation

#### 4.3 IPv6 Planning

For the AfgREN infrastructure it is very much important to be ready for the IPv6 deployment. The IPv6 addressing plan requires a very thorough and careful planning. Following are the main issues that will have to be considered for the IPv6 deployment.

- **Preparation and Planning**
  - Initial Discussions started
  - Follow up discussion required
  - Trainings and workshops for the technical staff required

- **Compatibility**
  - Existing equipment compatibility should be verified
  - All new equipments should support IPv6
  - Service Providers should be capable of routing IPv6 traffic

- **Implementation**
  - Can be implemented in several phases
  - Phase 1 small universities
  - Phase 2 medium size universities
  - Phase 3 large universities
  - Parallel running of IPv4 and IPv6 will be required

*Figure 5 IPv6 Planning*
4.4 Bandwidth Requirements

The bandwidth requirement for each university varies and the initial requirements are not that high but to plan for a good and scalable infrastructure, the proposed bandwidth allocation for each university is shown in Table 2. Considering the ISPs and TSPs type of services availability, more than one option has been considered for each type of institution.

<table>
<thead>
<tr>
<th>Type of Institution and Connectivity to NOC</th>
<th>Type of Connectivity Option 1</th>
<th>Type of Connectivity Option 2</th>
<th>Type of Connectivity Option 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kabul-based Universities to NOC</td>
<td>1 Gigabit Metro Ethernet Fiber Optic Cable</td>
<td>155 Mbps (1x STM 1) Configured as DPLC</td>
<td>None</td>
</tr>
<tr>
<td>Large Provincial Universities to NOC</td>
<td>155 Mbps (1x STM 1) Configured as DPLC</td>
<td>51 Mbps (1x STM 0) Configured as DPLC</td>
<td>34 Mbps (1 x E3) Through PtP Fiber</td>
</tr>
<tr>
<td>Small Universities to NOC or Regional Univ.</td>
<td>34 Mbps (1x E3) Through PtP Fiber</td>
<td>34 Mbps (1x E3) Through PtP Microwave</td>
<td>10 Mbps (5x E1s) Through PtP Fiber or Microwave</td>
</tr>
<tr>
<td>Universities sub-campuses to Main Campus</td>
<td>34 Mbps (1x E3) Through PtP Fiber</td>
<td>10 Mbps (5x E1) Through PtP Fiber or Microwave</td>
<td>6 Mbps (3x E1s) Through PtP Fiber, Microwave or satellite</td>
</tr>
</tbody>
</table>

4.5 Monitoring and Reporting

In order for AfgREN infrastructure to be successful it has to be properly monitored and maintained. The AfgREN NOC staff should be able to monitor the entire AfgREN backbone 24/7 and generate required reports that can help in taking proactive and reactive actions, identifying problem areas, decision making, and planning for network improvements. Following are the list of main features that the AfgREN monitoring system should provide:

- A centralized networking monitoring system (NMS) is required at the AfgREN NOC to monitor the backbone links. Besides a small scale monitoring system is required at each university which will enable the IT managers to monitor the in-campus infrastructure.
- All equipments should be monitored using the in-band management method.
- Universities may require separate hardware in order to report bandwidth usage, traffic flow information, IPS logs and other security logs [7].
- The Management Information Base (MIB) of the management/monitoring system should be implemented into a separate system than the NMS itself, in order to answer to growth requirements.
- Redundancy and backup hardware and software should be included in the solution for the critical NMS components, like database servers and web applications.
- The NMS should be able to provide customized reports in addition to some of its default reporting templates. Reports should be exportable to email, PDF, Excel and CSV formats.
- The solution should show network devices and hosts resource usages like CPUs, Memory, Ports (interfaces), fans and disk usage. It should also show bottlenecks, top talkers, devices availability, bandwidth usage, downtime and delay.
- The NMS should provide the facility to define thresholds and send alerts if the thresholds are exceeded.
- The system should be capable of sending alerts using email, SMS, web alert, Popups and sound.
- The NMS should allow creating customized views for each campus network. Users’ access and permission should be restricted based on the views.
- The NMS interface should be web based, graphical and accessible from anywhere within the AfgREN Intranet and the Internet and it should have a dashboard manager.
- The solution should be able to monitor firewalls, IPS systems, IDS systems, routers, switches, servers, services, UPS, Wireless Access Points through SNMP v3 protocol. And the Unix and Linux servers through SSH or netmon.
- The solution should be able to analyze traffic flows of every application using xflow.
- The solution should be implemented on an IPv4 platform, but it must support IPv6.
- The solution should be capable of discovering and drawing the network topology by itself, it should allow the NOC staff to create device dependencies manually.
- The solution should consider installing video wall at the AfgREN NOC which will be the main NOC.
- The solution should also consider installing a small scale monitoring station at the MoHE-NOC with a summarized view of the AfgREN critical components for the monitoring purposes.

4.6 Security and Management
The AfgREN infrastructure must be safe environment for its intended user groups and it should also not be used as a platform or proxy network to attack other external networks. AfgREN should also form a Computer Emergency Response Team (AfgREN-CERT). This team will be responsible for responding to the security threats and coordinating security incidents with Afghanistan-CERT at MCIT and other organizations. The entire AfgREN Infrastructure must be secured using the various security products and best practices. The infrastructural equipments should be properly managed and access to the critical devices must be limited to the authorized AfgREN staff only. Keeping all this in mind following should be considered in order to ensure a secure and manageable infrastructure:

- An AAA (Authentication, Authorization and Accounting) system for each institution’s campus and sub-campus infrastructure with its required components (hardware, software, licenses, etc) is required [8].
• The AAA system should be implemented for the wired, wireless, networking equipments and end-user equipment. An AAA solution should be considered at the Main NOC for the purpose of authenticating and authorizing system administrators’ access to the networking devices with assigning different privilege levels and roles. These administrative roles should be assigned centrally through the AAA servers.

• The NMS solution should be able to receive process and analyze Syslog messages received from the Universities edge routers, firewalls and IPS systems on a centralized graphical user interface at the Main NOC. The NOC manager should be able to remotely administrator the edge devices.

• For the in-campus networking equipment Syslog messages and monitoring information should be sent to a server located at the campus and the view should be provided to the campus IT manager and he should be able to remotely administer the in-campus networking devices.

• The campus security devices should be capable of providing IPS, IDS, firewall, content filtering, URL filtering, antivirus, anti-spam services [8]. These services can be integrated in one single device. The security devices should be configured to send Syslog messages to Syslog servers either located at the campus or the main NOC for further analysis.

5 Sustainability
One of the main concerns of the International community specially the NATO Public Diplomacy Division, European Union and the US embassy is the sustainability of this project. Since as the funders and supporters of this project they may not be able to continue supporting this project forever. Therefore much contribution is expected from the MoHE’s management and the universities in order to make this project turn into a program and become self sustainable. For the sustainability of this project some of the main factors are the financial support, human resource, and proper maintenance of the infrastructure as shown in Figure 6.

While the International Community’s help and support is greatly appreciated, we expect their continuous support till this project becomes more sustainable. Considering sustainability as the key to the success of this project, MoHE has taken the first steps towards making this project sustainable by signing a Memorandum of Understanding (MoU) wit MCIT [3]. This MoU is meant for two purposes. The first purpose is to use the Telecom Development Fund (TDF) operated and controlled by ATRA to pay for the one time connectivity costs as part of the Tele Education Projects. And the second purpose is to provide long-term financial support for the AfgREN’s expansion and survival. This process has already started and several universities are connected and will be connected using these funds. For the recurring bandwidth cost payments the discussion are currently going on with MoHE, MCIT, ATRA and AFTEL.
Although using the TDF is a good solution towards making this national project sustainable, a stronger and long-term step could be taken by MoHE to include the AfgREN expansion and one-time costs in its Annual Development Budget and the recurring cost in its Annual Operating (Normal) Budget. This will guarantee the AfgREN’s infrastructure’s operation, continuation and institutions dependency will increase [4]. This sustainability step by MoHE doesn’t have to cover all the AfgREN associated costs at once, but MoHE can start by co-funding this project with other stakeholders, like NATO, European Union, US-Embassy and MCIT. For example MoHE can start with a co-funding of this project in 2014 with 20-30%, and it should be increased gradually. Within 4-5 years time 80-90% of the cost should be covered by MoHE internal budgets.

6 Milestones
There are various important factors that can affect the success of AfgREN are shown in Figure 7. The major factors that are identified as milestones are as listed below:

- Long-term financial support; commitment from the International donors and government
- Human resource required to run AfgREN infrastructure. Paying competitive salaries to managerial and technical staff.
- Legal framework for the AfgREN’s operation [4]
- Infrastructural readiness to run AfgREN. Addressing issues like human resource, proper campus networks and stable power.
Other factors that affect the AfgREN infrastructure are identified as following:

- Training the university’s academic staff, employees and students to make use of the ICT services
- Introducing computer aided trainings
- Introducing IT services that can positively change the teaching and learning environment using other development programs.
- Capacity building programs for the AfgREN managerial and technical staff
- Promoting research and development by creating public and private sector partnerships

7 Conclusion

AfgREN has been identified has one of the main pillars and drivers of modern higher education system in Afghanistan. Its existence and operation is vital and promotes research, development, teaching and learning. The way the universities are currently communicating to each other and connected to the Internet should change. In order to form a realistic and effective National Research and Educational Network the physical topology, logical topology, IPv6 planning, bandwidth allocation, monitoring and security aspects should be considered well in advance. The proposed infrastructure for AfgREN considers a central NOC based at Kabul University, 1 Gigabit Metro Ethernet or 155 Mbps links for Kabul-based Universities, 155 Mbps dedicated links for large provincial universities, 34 Mbps for small universities and sub-campuses. The AfgREN infrastructure should be designed based on hierarchical design model, which will increase the network performance, security, manageability and availability. The infrastructure should also be ready to accept new technologies and protocols like IPv6. The sustainability of AfgREN could be guaranteed by donors and supporters long-term commitments, and MoHE’s initiative to include the associated costs in its annual development and normal budgets gradually. The milestones for the AfgRENS success is identified as long-term stakeholder’s commitments, legal frame work, human resource, infrastructural improvements, MoHE staff capacity building, IT trainings and effective services delivery.
8 References

4. DYER, J. (2009), The case for National Research and Educational Networks, Netherlands: Tarena, pp 5, 7, 10, 12