Date: 5.May.2007

BROADBAND NETWORK DESIGN
Proposal

Done by
Mohammad A. Mikki

Dear Dr. Foad El-Harazin

This proposal is submitted to Global Peace Through The Global University System (GUS); and Palestinian e-learning and e-healthcare/telemedicine project for a Broadband Network Design and Telecommunication services. Our scope has been structured in accordance with our recent discussions with Dr. Foad El-Harazin.

Dr. M. Mikki will provide engineering design and consulting services to connect all GUS buildings and establish a broadband network for the whole project. The broadband network will be capable of providing digital voice, video and other multimedia data services. The network will also support wireless technology platforms and applications.

Should you have any questions or require additional information, please feel free to contact me anytime.

Sincerely,

Dr. Eng. M. Mikki

Need of Broadband Networks

Information technologies provide opportunities for improved and more flexible working methods in organizations. In particular, the provision of a broadband network infrastructure is an important element in e-learning/e-healthcare applications that require the exchange of complex multimedia documents and for integrating many business-to-customer and business-to-business services. The development of broadband networks could serve to improve the competitive equilibrium between educational institutions in Gaza Strip/West Bank and their competitors in rest of the world. We address the issue of the need broadband access.

Background and Primary Goals

Universities today are motivated to subscribe to broadband networks. This motivation is based on the common belief that high capacity telecommunication networks are essential to support services that require the exchange of complex multimedia documents and for integrating many business-to-customer and business-to-business services. Simultaneously, universities in Gaza Strip/West Bank communities meet many competitive challenges of having traditional and e-learners, faculty and employees dispersed over large geographic distances. This matches well with the view of the European Commission, which has initiated several research programs in order to improve the competitive skill for European companies. The IST program (Information Society Technologies) has set up a group of projects under the heading Key Action II: New Methods of Work and Electronic Commerce, which in February 2000 accounts for 88 different projects. The goal of the Key Action II initiative is to "develop information society technologies to enable European workers and enterprises, in particular SMEs, to increase their competitiveness in the global marketplace, whilst at the same time improving the quality of the individual's working life, through the use of information society technologies to provide the flexibility to be free from many existing constraints on both working methods and organization, including those imposed by distance and time."

This is also the motivation behind the broadband initiative of the central government in Norway and the initiative for an increased use of electronic commerce and electronic business. In the eNorway 3.0 document the following goals are expressed:

- "ensure that a majority of Norway’s municipalities take use of broadband services, not just an active minority
- avoid differences arising between central and less central parts of the country. "

<u>Design Services</u>

1. Fiber Optic Backbone
2. ADSL-based broadband network
3. Wireless technology -based broadband network
4. Any other technical Services

Tasks

The network will include a fiber-optic cable backbone encompassing the Gaza Strip area. The network will support direct connections to buildings and educational facilities. The Metropolitan Area Network platform will provide the availability and delivery of all voice, video and other multimedia data services over the fiber optic backbone.

The following presents the proposed tasks in detail:

Task 1: Consulting Services

1. Assist the GUS personnel to prepare the technical part of he proposals documents
2. Assist with estimating financial budget and cost of various parts of the project.

Task 2: Fiber Optic Design

Develop a detailed design to establish fiber-optic cable routes within the city of Gaza and the other cities, camps and villages of Gaza Strip. This design will include:

1. Identification of bundle sizes and potential terminations, splices and breakout points
2. Detailed design of the initial fiber backbone segment
3. Identification of demarcation points at each location
4. Preparation of equipment list and materials
5. Design provisions for future expansion within geographical areas limits

Task 3: Network Design

Assist in the detailed Network design. This includes:

1. Specify equipment
2. Consideration of space requirements for facilities to house the electronic equipment and the required environment to meet the equipment's specifications
3. Assist in the development of selected user locations, interface equipment, and networking platform for the delivery of high-speed data transmission services.

4. Recommendations on the operating platform gear and network monitoring system

5. Recommend network and systems integration

6. Provide equipment estimates

Task 4: Easement and Right of Way Assessment

This task will include the identification of easements and ROW required over the entire network route. This will provide design criteria and drive-out distribution system routes.

1. The identification of available underground conduit and requirements for new underground construction

2. The identification of available aerial conduit and/or plant facilities for network equipment.

Task 5: Project Management

1. Providing overall technical part of project direction

2. Assist with document preparation

3. Coordinate all external and internal technical communications

4. Coordinate all work associated with contractors

5. Distribute all necessary project related documentation.

Task 6: Services during Construction

1. Provide consultation services during construction, answer questions, etc.

2. Meet periodically with the contractors to provide general project management assistance.

Appendix A:

Wireless Network Architecture

Driven by standardization, widespread vendor adoption and ease of use, we could use the technical option to implement a wireless broadband network that supports delivery of online lectures and e-healthcare applications with minimal complexity and associated client costs. With this intent, it is important that the network work seamlessly with standard 802.11b (WiFi) clients.

Mesh network architectures seem to provide the best solution for metro-scale wireless broadband networks. If a mesh architecture solution is not provided, we could present other architectures as opposed to mesh architecture.

Some key factors to use mesh architecture are ease and cost of deployment, scalability, network access points, network node-to-node interface and range, and compatibility with 802.16 standards.

Carrier-grade Coverage and Resiliency

Network reliability is an essential requirement for the educational and healthcare applications that will grow to depend on this network. The proposal recognizes that Wi Fi transmissions are prone to temporary localized interference that is unpredictable in nature. For this reason, it is important that the solution provide network-layer resiliency and self-healing features that enable the technical architects to design a network to the GUS's required level of system availability.

Network Management and Security

The security of 802.11 wireless networks is of serious concern. Numerous observers have highlighted the potential vulnerabilities of standard 802.11 wireless networks. It is essential that the solution closely follow the strongest industry recommendations for securing wireless networks.

The proposed solution will employ the following industry security recommendations and guidelines:

- **Multi-layered** — Utilize multiple security mechanisms at several network layers to provide high levels of protection.
- **Time-tested and proven**—Utilize security techniques that are well-known and trusted.
- **Open, standards-based**— Integrate elements that have undergone extensive scrutiny by the security community and can offer users a strong degree of confidence in their implementation.
- **Upgradeable** —Because new security threats often emerge, any architecture must be upgradeable to eliminate future security holes.

The task of securing wireless networks can be divided into five challenges:

- Network access control through authentication—Wireless network security begins with prohibiting access by unauthorized wireless devices.

- Protection of wired assets from malicious wireless clients—Because the goal of a wireless network is to provide access to a network of wired devices (servers, printers, databases), a wireless network deployment must carefully protect those resources from malicious users.

- Protection of wireless clients from other malicious wireless clients—Wireless clients must be protected both for their own sake and to prevent a permitted client from being used for access by an unauthorized client.

- Secure end-to-end transmission of sensitive data—Because malicious users can sniff the airwaves, data traffic traveling over the wireless network must be shielded from eavesdroppers by a strong encryption algorithm.

- Secure network configuration and management —To prohibit sophisticated hacking, it should not be possible for anyone but authorized network operators to alter the operation of network elements or the network's path selection protocol.

The broadband study includes a customized broadband network design Gaza Strip/West Bank. We start by collecting data on existing infrastructure and basic requirements for data communications. We then design a system, evaluating the most compatible technology using state-of-the-art propagation and dimensioning tools. We design the system for e-learning/e-healthcare services – using redundant components and worst-case scenarios

Appendix B

ADSL Solution

Introduction and Scope

This appendix recommends a set of interoperable Core Network Architectures to support broadband service over ADSL systems, and specifies minimum requirements for each. Each of the network architecture is based on the PPP over ATM (over ADSL) model.

Network Services and Applications

The principal requirements of the Core Network Architecture recommends PPP over ATM (over ADSL) as the user plane protocol independent of transmission layer line code at the U-interface.

The scope of this appendix is to specify recommendations as to the Core Network infrastructure, its associated protocols and interfaces beyond the U-interface to support the customer premises for application to access the legacy network. There are two key issues in development of a CPE Architecture solution. One is whether multiple PCs will be interconnected sharing a common high-speed data pipe or if it is only a single PC connected to the high-speed data access, and the other is the type of applications the end user is expected to use.

These two variables generally separate residential and SOHO data accesses to the Core Network into the following scenarios:

- Sessions to individual applications
- Multi-homing of individual applications
- Multiple sessions to single NSP
- Simultaneous sessions to multiple NSPs

Support for sessions to individual applications is accomplished by transporting PPP from the end system (e.g., PC) across the U-interface to enter the Core Network. One VC is mapped to one PPP session.

Multi-homing of individual applications is a mechanism whereby an individual end system may support more than one PPP session. In this scenario, the corresponding VCs are provisioned for each PPP session. Nevertheless, it may be desirable for the Core Network, at some point, to support the termination function of multiplexed PPP sessions over a shared VC1.

Multiple sessions to a single NSP allow multiple end systems to share a common link to an NSP through an aggregation function (bridging or routing) function in either the B-NT or a proxy. This means that one or more subnets in the premises on the same Layer 3 network all have logical connectivity with an external Layer 3 network, i.e., NSP. Therefore, it is desirable for the Core Network to support

the aggregation function where the PPP session is terminated in the Core Network.

Simultaneous sessions to multiple NSPs allow a single user or multiple end systems on a CPE network to have active sessions with different NSPs simultaneously. Some form of Layer 2 multiplexing may be performed at the premises in order to allow multiple Layer 3 domains to be simultaneously supported. In this scenario, it is desirable for the Core Network to be able to support the session aggregation function to interface to multiple NSPs. However, there is a potential security problem, especially when one of the NSPs is a corporate network.

The access scenarios described above demand that a Core Network support:

- Bulk provisioning.
- Mechanisms to ensure privacy of user data.
- Aggregation of traffic from multiple Access Node and delivery of the aggregated traffic to the NSP. The aggregation may or may not involve statistical multiplexing.
- Proxy Authentication, Accounting, Addressing and Authorization on behalf of the NSP.
- Quality of Service objectives and/or service level agreements.

Access Configuration
The ability to provide services to a large population of customers plays a key role in deploying ADSL services including Internet access, corporate network access, local content and peer-to-peer communications.

The Core Network operator must be equipped with effective tools to support the service provisioning and selection between the Service Provider and the user.

The service provisioning must exist between Service Provider and end user. The mechanism of transporting the service provisioning information to a user should be automatic without the user's intervention, so that user can access a service offered by an NSP based upon the received service provisioning information.