

3.0 Communications and Networking

Dr. Vincent Chan

With the disappearance of the USSR as the major strategic threat to the U.S., the most likely foreign crisis for the U.S. in the future will be regional (likely third world) conflicts that threaten our interests overseas. Since these conflicts can occur anywhere geographically, there is the need for a global defense network that can provide instant connectivity to surveillance/reconnaissance assets, rapid deployment forces and other military assets in a newly formed theater-of-operation, as well as in CONUS.

Applications

Future information infrastructure should have global reach and will be comprised of an interconnection of multiple, sometimes very disparate, communications systems or networks, some of which will be new and some which will include heritage systems in existence or planned to be deployed in the near future.

Concept (Tactical Theater Operations)

Components of these systems include: (1) satellite communications systems for the relay of very high data rate sensor-data, including downlinks; (2) military and commercial SATCOM systems (such as Milstar, DSCS, GBS, TDRSS, INMARSAT, etc.) for voice, video and data communications; (3) mobile SATCOM terminals for aircraft, ground forces and ships; and (4) a global reach ground network infrastructure that includes military and commercial networks. A special architecture will have to be developed for the proper internetting of these systems to provide an efficient infrastructure for data collection, voice, video and data traffic, intelligence data and map dissemination, precision-target and navigation information, messages providing classification/identification of friendly and enemy fixed, mobile and moving targets and command and control messages. This communication/network system should not impair mobility and should provide: (1) global coverage, as well as (2) coverage over any potential battle theater.

Figure 12. depicts the concept for a global network in support of tactical theater operations. Functionally, this information network must maintain connectivity with our forward assets, CONUS sites, other services and our allies. This requirement for connectivity is functionally shown in Figure 13. This network will include DoD developed systems as well as commercially purchased or leased systems. Since in a theater operation scenario, the geographic location of the theater may not be known well ahead of time, the defense network must not only provide instant connectivity to a sudden increase of users and user types but a surge in the capacity of the connections as well. Traditional DoD connectivities today are mostly by circuit switched voice service. In the future, data services will be more important and large number of users will have to be served by, in some cases, very precious resources. So sharing of resources via multiple random access of the network infrastructure will become an important aspect of the defense network. This would be a paradigm shift for the DoD and it behooves the Air Force to start this very important development and build up process by investing in the creation of the appropriate architecture.

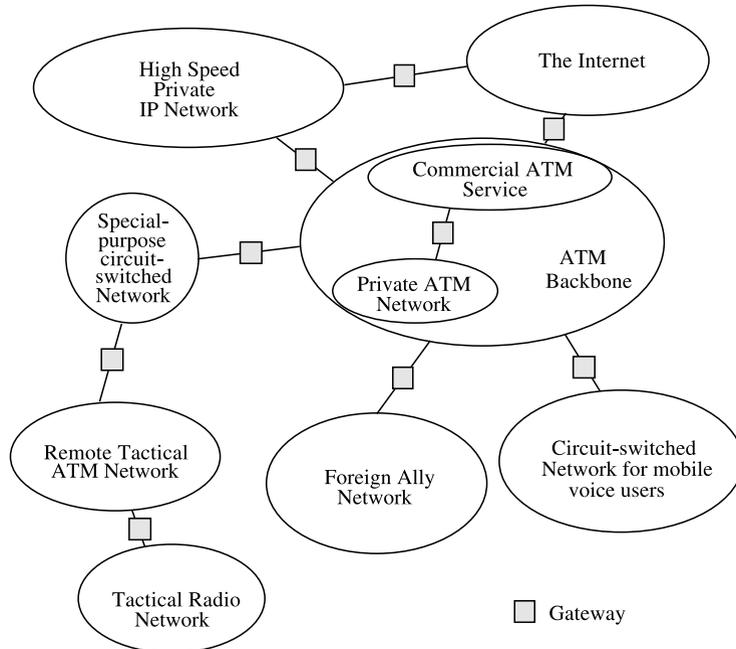


Figure 12.

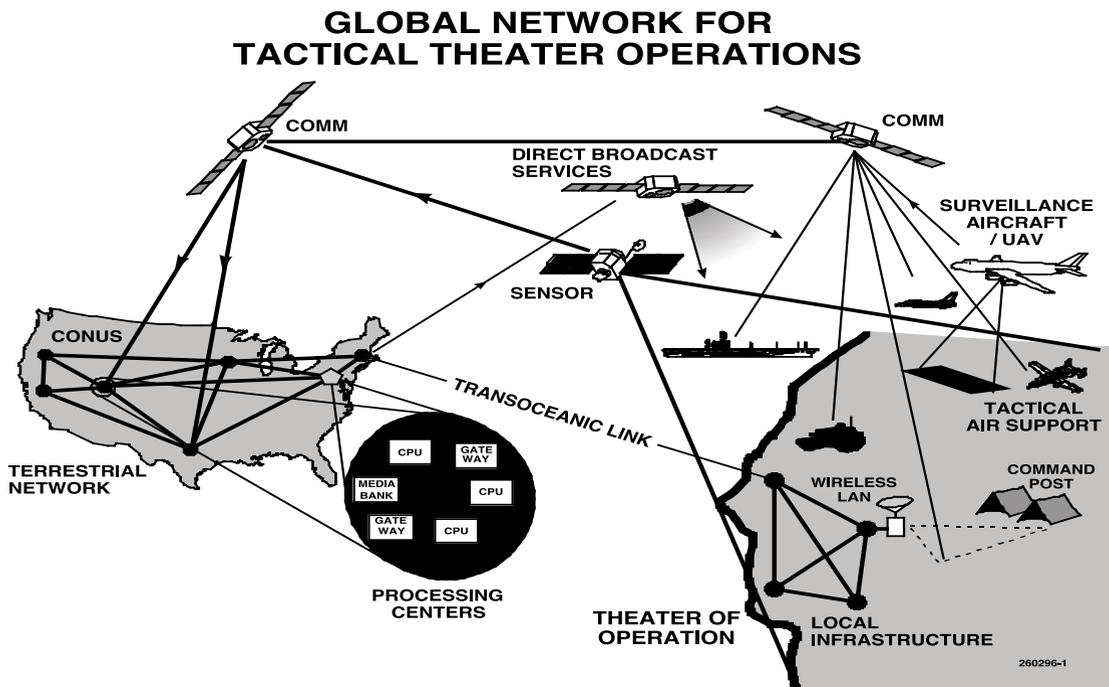


Figure 13. Global Networks for Tactical Theater Operations

Protected Core and Soft-Shell Network

With the rapid maturity of information and communication technologies world-wide, it is safe to assume that today's advance technologies will be available to our allies as well as our adversaries in the years beyond 2000. In fact the differential between US and foreign communications technologies will be closing with the rapid dissemination and deployment of commercial technologies, systems and services. Thus, it is imperative that the Air Force, in conjunction with other DoD partners, develop for its future a world-wide network with a protected, fully connected sub-network core that it can rely on for its war-fighting situations, even though part of the larger network (the soft-shell) can be denied due to electronic or physical attacks. In peacetime, the convenience of the larger capacity network can be used; but the war-fighting units must learn and practice to operate with the reduced capacities as well. Since highly protected communications services are expensive, high rate services may not be available to every user connected to the network. Thus, some units may have to operate based on protected message services only, rather than video or even voice connectivities.

While it is reasonable and pragmatic to assume the soft-shell outer network will be comprised of commercial as well as DoD developed systems, the protected inner core must have specially developed DoD systems and when commercial technologies or services are used, special DoD developed architectures must be employed to decrease the vulnerability of such systems. (An example of a more survivable ground network based on commercial fiber technology is one that uses multiple diversity paths albeit at increased expense). In addition, the critical irreducible information exchanges and connectivities for theater operations such as warfighting should be characterized and quantified. The core network must be designed to provide, at a minimum, those services even in the presence of a state-of-the-art physical and electronic threat. The network architecture must ensure the proper quality of service (QOS) is delivered to critical users of the network. Some of these QOSs are: deadlines for message delivery, time and location tacking, low error rates for data and low latency for interactive voice and video services. High QOS is hard to achieve with ad hoc network architectures. The Air Force together with its DoD partners should develop a totally rational architecture based on user requirements and what technologies can support. With current technologies, there will be some weak links (as discussed below). Possible system development paths to improve survivability should be identified. Since the threat level that will be experienced in a future conflict is highly dependent of the adversary's technological maturity, the DoD network architecture should be one that can sense its environment and adapt its connectivity and capacity accordingly.

Service Types, Connectivities and Capacities

In future everyday Air Force operations and theater operations there will be significantly increased dependence on network services. Many of these services and connectivities will be new. It is probably useful to think about the necessary architecture by attempting to organize these services and connectivities, and their associated capacity requirements, into various classes (Figure 14 gives a graphic view of the necessary connectivities).

- *High Speed Trunks*: These will be used for data collection, dissemination, trunking of aggregated traffic (such as those between ATM switches), and large volume data broadcasts. These trunks most likely will be primarily fiber and in special cases via satellites for mobile connections and diversity protection. The data in

each trunk can be as high as 10's of Gbps. The connectivity requirement for this type of service consists of two types: (1) routine, slowly changing connections that make up the bulk of routine DoD usage globally (therefore a global extent), and (2) sudden surge of connections into a theater of operation at the beginning of conflicts (and therefore must be mobile and be capable of instant set-up).

- *Links Between Large Airborne Platforms and Command Posts /Control Centers:* Critical connectivities between airborne sensors (e.g. JSTARS, Rivet Joints, U2 etc.), airborne and ground based command/control centers must be maintained. This can be done by SATCOM or by some future in-air microwave networks. Types of services will include high rate data streams (can be as high as Gbps), voice circuits and multiple access datagram services.

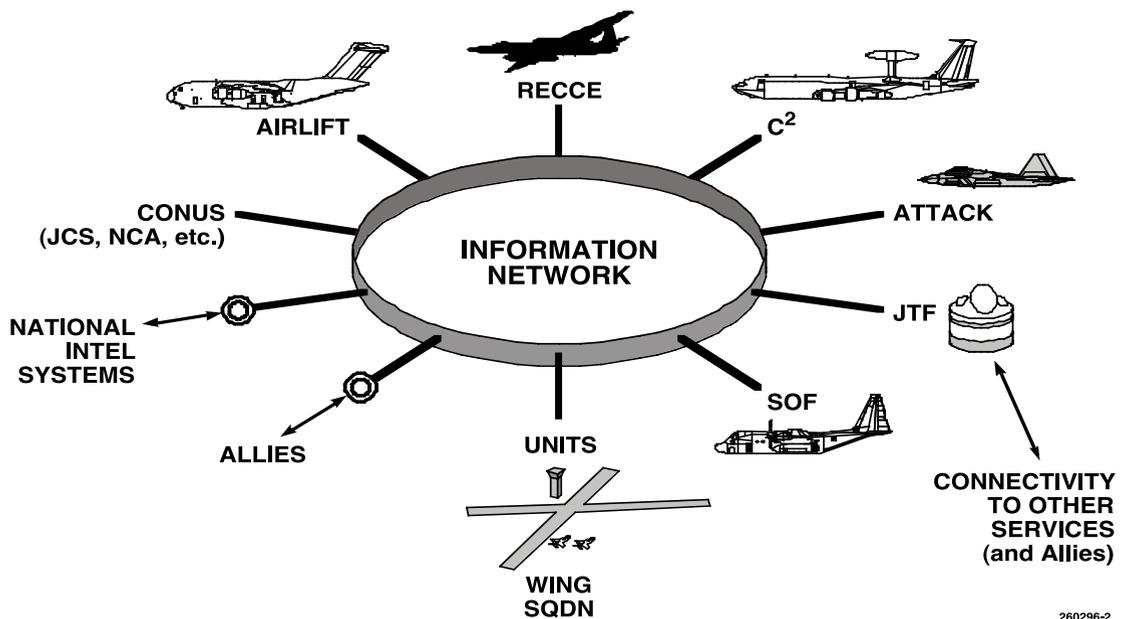


Figure 14. Connectivity Requirements for Future Air Force Communications Network

- *Broadcast Services from Satellites and Aircraft including UAVs:* Maps, intelligence products and situation awareness reports will be broadcast to the theater via SATCOM or airborne assets including UAV's, and direct from sensor aircraft such as JSTARS and Rivet Joint. The amount of data in the broadcast can easily reach 100 Mbps to 1 Gbps in the future, even with custom request data-pull from users. In the case of tailoring to specific user request for sending data in a broadcast, there should be at least a low rate return link from the user for acknowledgment of packets in the transport protocol. This return link is indispensable for critical message deliveries.

- *Connections between Fighters/Bombers and Command/Control Centers and Airborne Sensors:* This is the critical link by which the fighters and bombers can retain connectivity with the theater command and control infrastructure and also receive updates of situations and intel-products. This type of connection is typically very difficult to accommodate due to the limited space available on the aircraft for antennas, cost issues and the desire for the aircraft not to be detected via its transmitter emission. In this case, data service may be more important than voice service. Links of data rates up to Mbps can be required between airborne and ground entities even with significant data compression employed. In addition, there should be receivers for satellite or UAV broadcasts at 10's of Mbps and a low rate return link for acknowledgments if critical messages are to be sent via this mode. If on-board sensor data is to be shared among wingmen and also sent to theater rear, links originating from the fighters and bombers of Mbps class will be required to support such a mode of operation. Otherwise, lower rate data links will suffice.

There is a very important trade-off that the information infrastructure designer has to be aware of throughout the development process and that is: there is a significant trade between processing power and communication data rates. For example, more fusion and decisions at the sensors and the command centers will lower data rate requirements to the aircraft. Whereas for terrestrial fiber connections the cost of transport can be so low that a lot of compression and preprocessing may not be required. It is much too early to perform the trade at this point in time. The network designer should be conscious of this issue and the trade will evolve as the two technologies will in the next decade or so.

Satellite Communications

SATCOM is a critical element for providing connectivity to mobile and transportable military users in support of long range missions and theaters of operations.

General Perspectives

Current DoD SATCOM and commercial SATCOM can be utilized to provide connectivity. The DoD SATCOM systems operate at UHF (250 to 400 MHz) for low rate (up to 9.6 Kbps) unprotected communications to mobile users; at SHF (8/7 GHz) for low to high rate (up to 10+ Mbps) protected communications to fixed and transportable users; and at EHF (44/20 GHz) for low to medium rate (up to 2 Mbps) highly protected communications for mobile users. The services provided on commercial systems range from low rate services to mobile users at L-band to high rate services to fixed and transportable users at K-band. The key challenges which must be met to provide better SATCOM support to the tactical forces include inter-networking, increased capacity, and affordability. Inter-networking is required to bridge between different tactical SATCOM users via gateways between DoD and/or commercial satellites and into the terrestrial network. Increased capacities are needed for the military SATCOM links to support higher rates from mobile users and to provide increased global broadcast service (GBS) capabilities for information dissemination. Affordability will continue to be a challenge in an era of shrinking budgets and growing requirements.

There are major differences in the technologies and architectures of these military and commercial SATCOM systems. Furthermore, multiple administrative domains will be involved

in the construction and operation of the connected infrastructure, leading to a large degree of heterogeneity. These differences and the heterogeneous nature of the interconnected network lead to a number of technical issues which need to be resolved. These critical issues include internetwork gateway designs, network management and control, assurances of quality of service across subnetworks and network security and survivability. To create an affordable architecture is a challenging yet very important task. A substantial architectural design effort will have to be initiated in this area. A well thought out design with adaptivity and highly fluid interconnections can improve survivability, responsiveness and cost.

Protected and Unprotected Satellite Communication

Protected SATCOM achieves its effectiveness via a number of techniques: spread spectrum, anti-jam signal designs, on-board signal processing, spatial discrimination via shaped antenna beams and/or antenna processing (nulling). The Milstar EHF service is an example of a well protected SATCOM. With a combination of the mentioned techniques the Milstar system should be well protected into the 21st century, maybe with minor upgrades as technology develops in the next decade or so.

With the rapid advancement of commercial SATCOM technology and proliferation of commercial SATCOM services, it is reasonable to assume that SATCOM space and ground segment technologies will be widely available at a reasonable cost around the world at least by the turn of the century. At the lower frequencies (UHF, SHF), there will not be adequate bandwidth for band-spreading, and advanced adaptive antenna systems will be too large and costly to overcome commercially available jamming sources. Thus it should be assumed such services can be denied in the midst of a conflict with an adversary of moderate sophistication. Thus the Air Force might as well rely on commercial supply for these systems in the 21st century for cost reasons. However, these services and commercially supplied EHF can perfectly form the soft-shell communication network mentioned above, although multiple diversities of systems can decrease vulnerabilities some.

In the critical moments of a conflict, the Air Force must have reliable communication to its most important assets, such as sensors and airplanes. The protected core network should be designed to withstand reasonable projections of electronic threats. This system must have good anti-jam capability and low-probability of detection and interception. At EHF, 94 GHz and optical frequencies, there is enough bandwidth for spread spectrum or the frequencies are high enough to provide substantial protection via narrow beams or beam shaping. Again the Milstar system is a prime example of such a system, whereas there is little work done at 94 GHz and there have been many aborted unsuccessful efforts at optical frequencies. When the EHF frequencies become congested it is logical to move to these higher frequencies. Figure 15 attempts to put the many different DoD and commercial SATCOM systems in perspective.

Note that for world-wide coverage, these satellites must be interconnected via crosslinks or ground networks and gateways. When commercial technologies and/or services are used it is absolutely essential that such interconnection does not decrease the protection of such a system. Indiscriminate use of commercial fiber services, for example, may present unacceptable vulnerabilities to physical and electronic attacks. In this case, the commercial services should be considered unreliable and if needed a reliable architecture can be created over this unreliable

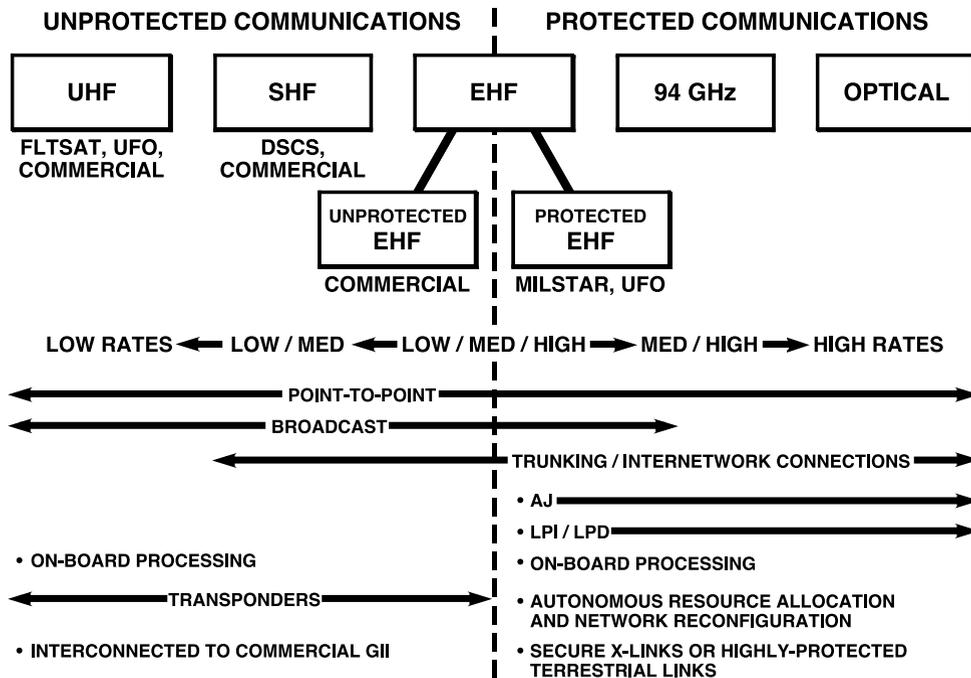


Figure 15. SATCOM Systems

substrate. This would require significant architectural development and higher deployment costs, which should be traded off against the costs of crosslinks.

EHF and Higher Frequency SATCOM for Aircraft

Many types of Air Force aircraft would function well with just protected critical message communication capability. Higher bandwidth voice and video are conveniences but probably not essential. This is fortunate since the cost of highly protected communications even at low rates is very high. EHF and higher frequency systems can provide anti-jam and low probability of detection and interception. Technology development in the next two decades should strive for low cost aircraft terminals. The enabling technologies include: solid state power generation, lightweight conformal phased array antennas and an architecture for sharing the channel medium efficiently for packet services with QOS peculiar to DoD, and specifically Air Force, applications.

One big stumbling block for the introduction of SATCOM into a small aircraft is the intrusiveness of the antenna, especially at high frequencies where antenna gain, LPI and AJ make their use inevitable. Current dish antennas are big, heavy and difficult and costly to integrate onto an aircraft. The enabling technology of the future will be the conformal phased array antenna that can be placed on the skin of the aircraft and the antenna beam is steered by electronically phasing the individual elements of the array. Present generations of phased array antennas use waveguide or free space propagation to feed the individual elements with their signals from a central processor. Unfortunately, these feed structures tend to be too thick for easy integration

onto the aircraft. Using fiber optics technology will make the feeds smaller and lighter. With this technology, the RF signals are modulated onto an optical carrier for transmission and converted back to microwave signals at the array elements. In an advanced form of this technology, optics can also be used to provide the processing and phase shifting functions. Research in this area has just begun, but it should be ready for deployment by the next millennium.

Intra-Flight (Air-to-Air) Communications

In addition to SATCOM to provide reach back and global connectivity for aircraft, there is also the need for intra-flight communications. Currently used UHF and planned EHF systems either have too low rates or their emissions can be readily detected at a distance and the aircraft located. Also some of these systems were designed before the rapid development of data networking and it is very difficult to interface these systems with other data networks. In most cases standard higher layer protocols cannot be simply applied. These problems will be further accentuated when the data rate requirements move up in the future from Kbps to Mbps. In a few links, such as those among UAVs, AWACS, Rivet Joints, Airborne Command Posts and other larger platforms the data rates requirements between two platforms can be as high as 100 Mbps. In the face of these new data flow trends, two techniques seem promising and should be pursued to provide high rate covert intra-flight and other aircraft to aircraft communications. These are 60+GHz and optical technologies.

Bandspreading can be used on an air-to-air data link operating with a modest transmitter (~2 mw). A communication link using this power could carry at least 200 Kbps using two inch apertures to a range of 20 miles if operating at 60 Ghz. The data rate would decrease with range squared or increase directly with transmitter power. An intercept detector at a range of 200 miles having a detector aperture of two feet would require an integration time of 200 seconds for a reliable detection (assuming that it is in a sidelobe). This is operationally impractical. If the link operates at the right frequency at 60 Ghz, additional path attenuation due to oxygen absorption would make the detector's task even more difficult, if not impossible (consequently, more communication power can be used to raise the data rate and/or range). The link needs a rapidly steerable or adaptive antenna due to its narrow beamwidths. Either a phased array or small dish can be used.

Optical links are also a possibility for covert air-to-air links. There have been a number of systems tried experimentally. They would have the advantage of narrow beams which are hard to detect. Also atmospheric absorption lines are available to limit detectability due to rapid power drop-off with distance, in which case broad beams (even omni) can be used.

Optical Space Laser Communications for High Speed Data Relay

Laser crosslinks offer the promise of very high data rate capability (>10 Gbps) coupled with very small package size (<100 lbs) for point-to-point links. Moreover, the high transmitter power (>2 W) and quantum limited optical receivers that now have been demonstrated in the laboratory, can be used to good advantage for lower rate crosslink applications where extremely small packages can now be built (e.g., under 40 lbs for 10 Mbps). Additionally, lasercom links are attractive for other applications such as UAV-to-UAV relay and UAV-to-satellite relay where high speed (300 Mbps) links can be closed with aperture size on the order of a few inches.

In the past, DoD and NASA have invested in several aborted unsuccessful programs in lasercom. The reasons for these failures can be attributed to the lack of understanding and elegant engineering solutions to critical areas of spatial acquisition and tracking of narrow optical beams, high power transmitter and sensitive receiver technology, thermal/mechanical/optical engineering of the space-borne hardware and overall system engineering. During the past few years, research and development have advanced to the point where these critical issues have been addressed and lasercom deployment in the 21st century is an achievable goal with continued development.

Terrestrial Networks

Commercial fiber-optic communications is undergoing a tremendous revolution in the 1990's. New installation of the latest generation of technology world-wide has increased capacities manyfold.

ATM/SONET Technology

In the years beyond 2000, the ubiquitous fiber transport will be SONET (Synchronous Optical Network) of various rate starting from OC-3 at 155 Mbps to OC-192 at 9.6 Gbps (usually by a factor of 4 in capacity at each increment). Since this internationally agreed upon standard will be wide spread, the DoD network should use the same standard whenever possible. For subnetworks that for one reason or another do not use this standard, proper interfaces should be implemented to bridge the networks seamlessly.

While SONET is a technology suitable for trunking, an emerging standard, Asynchronous Transfer Mode (ATM), can be used with SONET as connecting links between ATM switches for the support of heterogeneous users with very different requirements for rates and quality of services. The use of ATM technology in the military communications infrastructure should provide a number of significant benefits. The characteristics of ATM (efficient multiplexing and unified switching) should allow the deployment of a cost-effective network while providing a wide variety of services such as voice, video, and traditional data transfer. These are the same benefits expected by the commercial users of ATM technology. Furthermore, the fairly rapid pace of standardization of most aspects of ATM should allow equipment from different vendors to interoperate while the large commercial interest in ATM will ensure a large vendor base from which equipment may be procured. This equipment will be suitable for both private and public network applications. Finally, ATM is planned as the underlying "bitway" technology used by many domestic and foreign service providers, and many of these providers are expected to offer ATM user services at attractive prices.

All-Optical WDM Networks

SONET is a well established commercial standard for high speed optical transmission. Some long distance companies are now deploying point-to-point wavelength division multiplexing (WDM) in conjunction with SONET in order to further increase trunking capacity. Several research organizations around the world are now developing even higher capacity optical transmission and networking technology. Local area networks with 100 Gbps or more capacity and wide area network capacities in excess of 1 Tbps are envisioned.

One very active DoD/commercial research focus in the US is WDM network technology. These networks are capable of "all-optical" operations in that within the network there are no

optical-to-electrical transitions that may “bottleneck” the speed of the network or limit its versatility. Due to the characteristics of optical routing and switching, these networks are also rapidly reconfigurable. This is a very attractive property for rapid connectivity and capacity adaptation for recovery after link failure and sudden surge of traffic due to quickly changing situations. The rapid switching and routing property will be especially useful for the introduction of fast rerouting of the network as a form of ‘spatial path hopping’ to decrease the vulnerability against physical attack of the network. In this technique a connection between two users are constantly changing over many possible paths by some schedule protected by means of a key. This would make interception and total denial by cutting a single or a few links much more difficult. The technique can be one of several that can provide a ‘reliable network over an reliable substrate’. In this case the unreliability stem from the adversary. Several fundamental and enabling technology components have been developed including: fast tunable transmitters, fast tunable receivers, wavelength sensitive routing elements, multi-wavelength switches, and optical frequency converters. This area of research may lead to the next generation of high performance terrestrial networks and become the backbone of the DoD global network in the 21st century.

All-Optical TDM Networks

Future military communications, supported by an integrated global defense network, will benefit from the ability to rapidly process, fuse and disseminate large volumes of data with low latency. For example, processing centers and data archives located generally within the same geographic area will need a high performance local/metropolitan area network for communications. For this application, ultra-high-speed optical time-division multiplexed (TDM) systems, operating at single stream rate of 100 Gbps, offer important operating advantages over other multiplexing schemes. These advantages include increased “intelligence” within the network to perform dynamic routing which enables packet service (a service generally more suitable for computer data communications) and truly flexible bandwidth on demand with low delay.

Several key enabling technologies for these high performance networks must be first developed. For high speed transmissions, these systems will rely on nonlinear optical pulse propagation (solitons). Various laboratories around the world have demonstrated 100 Gbps propagation over 100 Km. In addition, short pulse sources, pico-second class optical clock recovery, optical buffering and optical switching for packet processing need to be fully developed together with the creation of a network architecture suitable for ultra-high speed low latency operations.

Wireless

In many terrestrial applications, it would be difficult to install instant wired connections. Thus the role of wireless networking will be very important. Currently there is substantial research and development in the commercial sector in the area of digital wireless mobile phone networks. Some of these developing systems are perfectly suitable for adoption to DoD usage. These include the various forms of Time-Division-Multiplexed (TDM) systems, Code-Division-Multiplexed (CDM) systems and some Frequency-Division-Multiplexed (FDM) systems. With high probability, direct application of such wireless technology may not be possible because either some military environment is different or the DoD network to be connected to needs

protocol conversion at a gateway. Thus a well thought out architecture is needed before such adoption.

Less well developed in the commercial sector is wireless data networking, particularly at burst rates of 10-100 Mbps. Interactive data transfers among ground units will be used in a variety of ways that go beyond traditional command and control voice networks. Examples include: transmission and discussions of maps, intelligence and weather data, medical status reports and automatic geolocation reporting and monitoring. In these modes of operations, the network will have to support packet service for efficient use of resources. The user traffic will be bursty and unscheduled, but continuous connectivity is almost always required, even though the user can be mobile. The wireless environment will be harsh for data networking even for commercial applications. In DoD applications, protection from at least some level of jamming and interception must be provided via spread spectrum and/or antenna shaping techniques. Systems should be designed to adapt to the environment in data rates, modulation characteristics and spatial directivity. Smart (agile) wireless networks that apply to DoD usage will not be developed in the near term for commercial systems. Thus architectural design and technology development should be initiated in DoD-specific areas.

Architectures

In support of the information needs of new warfighting concepts, non-traditional data connectivities need to be established. There are a significant number of developments of new hardware and system concepts to bring more of a data networking approach to military communication. However, there is still much to be done to develop individual systems and integrate them into a seamless network.

General Perspectives

Advantage can be taken of the explosive development of commercial products and systems, but there are a number of unique attributes of military communication in the theater grid that will require new solutions and their integration with key existing systems. Among these unique attributes are: physical and electronic survivability as in low-probability of detection and interception, anti-jam, data security and ultra-reliable message deliveries with hard deadlines.

The network architecture should have a hard core that is well protected against threats and a soft outer shell that can provide higher capacities in benign environments. The network management system should be able to adapt real-time as threats arise and increase protection (at the expense of capacity) and/or reconfigure to maintain critical connectivity. There are a few choices available today for the interconnection of disparate networks. The Internet interconnects many disparate networks in a flat amorphous hierarchy. But that system would have a problem with critical message delivery with hard deadlines. ATM (asynchronous transfer mode) has been proposed as the format for world-wide internetwork connection. In this role, it will have many benefits. However, there are real differences in the requirements of military and commercial communications systems. Furthermore, multiple administrative domains will be involved in the construction and operation of this infrastructure leading to a large degree of heterogeneity. These differences and the heterogeneous nature of the internetwork lead to a number of technical issues which need to be resolved.

Some Differences between the Military and Commercial Communications Environments

While most of the services that must be provided by a worldwide military network are in common with the commercial environment, some are different:

- There are few needs for on-demand, multi-gigabit per second flows in today's commercial environment.
- Generally, in the commercial environment, demand for service evolves slowly allowing time for reliable fiber optic channels to be installed in time to satisfy that demand. This is not always the case in the military environment where there may be insufficient time or resources to install high quality channels and switching of sufficient capacity. Even when there would be time to install sufficient capacity, finite resources or other requirements may make it difficult to satisfy demand. For example, communications subsystems which have good anti-jam capability or low probability of detection are often only capable of providing a low bit-rate service.
- When a resource, such as bandwidth, is scarce, one or more users may be denied service by the network. Commercial networks try to avoid such a situation by over configuring their networks to reduce the probability of blocking and by tracking usage to plan for the installation of additional capacity. Therefore, they rarely need to deal with the issue of dynamically adjusting the behavior of the network to allocate scarce resources to high priority users at the expense of pre-empting others.
- User mobility/roaming is an issue that is only beginning to be addressed in the commercial environment. This has long been a requirement in the military environment.
- Even in applications where mobility were not an issue, the lack of physically secure terrestrial or undersea fiber to every area of operations implies more inventive use of the same medium or the use of other types of channels, such as RF and free-space optical, to connect to the backbone. These links span many orders of magnitude in link speed as well as bit error rate and have very different characteristics that have to be accounted for in the network architecture.
- The level of sophistication of (and resources available to) adversaries in the military environment implies much more attention needs to be paid to all aspects of security in a military network. This includes both physical survivability and electronic survivability and security.
- Often, special purpose communication links are needed which must be operated near their margin limits implying the need for extreme efficiency in link usage.
- Finally, in times of crisis, some minimum level of connectivity (availability), service, and performance must be guaranteed. Network operations and allocation of resources may be different when operating in such a mode. For example there should be a high degree of dynamic adaptivity unlike commercial systems.

Significant architectural efforts are needed, early on, to recognize these differences and account for them in an Air Force/DoD network architecture.

Multiple Network Types, and Multiple Administrative Domains

Today's military communications infrastructure is composed of many systems in various stages of their life-cycle. Because there is a large investment in these systems (people, process, hardware and software), we must assume that these systems will continue to exist for some time to come. Therefore, despite the desirability of a homogeneous ATM communications infrastructure, this will not occur for a number of years. This implies a period where end-to-end communications will occur over a hybrid (ATM and non-ATM) infrastructure. This leads to a number of technical issues which must be resolved.

The most obvious way to apply ATM is in backbones. ATM is well suited to this and appropriate channels will most likely be available there. This may be done with a) government-owned links, b) links leased from commercial providers, c) use of an ATM service from one or more carriers, or d) some combination of the above. Each alternative potentially has different implications on the management, monitoring, security, and routing of the network. The general strategy for resolving many of these issues is to use some form of gateway.

Even in the heterogeneous internetwork model, we should not, in general, assume a simple model in which only one ATM network is traversed by a given connection (see Figure 5). So, although we would expect non-ATM links would be primarily used to access an ATM backbone, this would not be their only usage.

Another key issue in this heterogeneous internetwork (HI) environment is the existence of more than one administrative domain. Each network shown in Figure 4 may be administered by a different entity - each with its own local goals, processes, policies, and *capabilities*. This factor will lead to a major set of issues which will need to be resolved for a smoothly operating (and useful) HI.

In addition, since ATM is designed for high rate fiber links, there are a set of issues involving how ATM will behave (together with higher-layer protocols) when used on non-fiber links such as SATCOM and wireless. For example, ATM does not do well over channels with low reliability and has no provision to accommodate changing network topology as in the case of mobile systems. Significant network architecture developments will be required to deal properly with these issues.

Protocol Development for Data Communications

The DoD has only just begun to incorporate data networking into their mode of operations. Hardware and software for computer communications is readily available in the commercial sector. While some of these products readily apply to DoD systems such as leased commercial fibers, other DoD communication systems will require network protocol development (especially the higher layer protocols). In many cases, the underlying links (e.g. SATCOM, wireless) are not designed for the algorithms used in these higher layer protocols (such as TCP). The reason is that many of the current DoD communications systems have been designed for circuit switched voice applications instead of data services, much less random access datagram services. It would require modifications of the links themselves, or the higher layer (transport/

network layers) protocols or the insertion of adaptation layers in between to provide the proper interface characteristics. These modifications or additions should not be ad hoc but should be designed to operate gracefully within the world-wide DoD network. Thus an early definition of a network architectural framework is imperative.

Summary

The Air Force's information network of the future should have global reach for its normal day-to-day operations as well as a capability that can allow an instant surge of connectivity and capacity into a localized theater for mobile and fixed-site users. The latter capability is perhaps the most difficult and costly to provide but yet is a very critical and important tool for tactical theater operations.

This information infrastructure will be extensive in scale and comprised of both military developed systems and commercial systems at various stages of their life cycles. The network will serve many functions but yet can provide ubiquitous connectivity via interconnecting of multiple (often disparate) systems. The major services provided should include: (1) data relay from spaceborne and airborne sensors, (2) SATCOM and other relay (as in UAV) services to mobile and fixed platforms, (3) a high speed terrestrial network infrastructure that includes fiber and land wireless systems.

Traditional DoD communication systems today mostly provide circuit-switched voice services, with fewer systems that are designed specifically for data transmissions. Data services will be used more in future applications and the service requirements will be different than those of voice only systems. Because of the bursty and unscheduled nature of data traffic, sharing of resources via efficient multiple access schemes will become an important characteristic of this network.

For the terrestrial network, significant use of commercial fiber and the new generation of digital wireless technology will lower costs. With the advent of wavelength-division-multiplexed (WDM) fiber networks, capacities of multi-Gbps per link will be available and affordable. Since commercial networks may not have the necessary reliability, various DoD specific upgrades, such as, spatial diversity transmission, traffic masking etc. must be used for critical services. WDM networks, for example, can allow rapid reconfiguration with little service impact via all-optical switching. Commercial open standards should be used for seamless operations.

Perhaps the most critical and difficult link in the Air Force network of the future is the high speed (1 Mbps) two-way access link to the aircraft. This link must support fairly substantial rates with low probability of intercept (LPI), little vulnerability to jamming (AJ) and also be easy to integrate at low costs. The key technology in this area is light-weight conformal electronically steerable phase array antennas (likely optically fed) at EHF frequencies and above with significant amount of bandwidth spreading of the waveforms used for LPI and AJ. This technology will have to be military driven, since commercial incentives for its development are not strong. While SATCOM will be the backbone of this system, a UAV intermediate relay can be a key element to lower terminal cost.

For the purpose of interconnection of networks, standard protocols should be used for interoperability and low development cost. However, current generations of higher layer protocols

that have been developed mostly for the fiber network, must be adapted to account for the less reliable and spatially changing links of mobile communications.

Since a significant amount of commercial assets will be used in the future Air Force network, the Air Force will have to deal with the vulnerability of these systems properly by creating a defense unique architecture that may use commercial transport as underlying substrates. The network should have a “hard core” that is well protected against various threats (physical or electronic) and a “soft-shell” that can provide higher/cheaper capacities in benign environments.

Research Threads for Communications and Networking

The AF should make maximum use of commercial technology and services. In addition, there are a number of defense-specific technologies that the AF should aggressively pursue:

- Low cost, LPI and AJ access links to airborne platforms at high rates (~1 Mbps), including optically-fed conformal phased array antenna technology, systems at new frequencies for more bandsreading, e.g. 94 GHz and 60 GHz(short range).
- High-rate optical crosslink technology for communication trunks and data relay.
- A defense-specific, reliable network architecture over unreliable substrates, creating an AF “hard-core/soft-shell” network.
- All-optical network (WDM/TDM) technologies for their potential in providing added survivability and security.

The Payoff to the AF Includes:

- A seamless world-wide network with the ability to deliver high-rate information in a timely manner to any user including airborne platforms.
- This network will adapt to various levels of threats and have the intelligence to provide critical connectivities even under the most severe attack.