Network Architecture Document:

"A Networking Framework for Delivering Business Results"

Version 1.0, May 2021

Prepared for:
Client Confidential

By:
Suresh Sundarrajan
Technical Writer

Network Domain Team Members

Confidential

COTS Enterprise Architecture Workgroup

Confidential

VirTable of Contents

Tables and Figures

Executive Summary

This document addresses network architecture recommendations for Client's agencies. The network architecture is part of Client's Enterprise-wide Technical Architecture (EWTA). The EWTA addresses the information technology requirements implied by the Client's business strategies and recommends related policies, standards, and best practices for Client's agencies.

The network architecture document is written to assist business and technical leaders in state agencies in making sound decisions related to networking. The document was drafted by the Network Domain Team, which was commissioned by the Enterprise Architecture Workgroup of the Council on Technology Services to provide network-related recommendations. The domain team identified local- and wide-area network (LAN and WAN) connectivity as the main technical architecture requirements. They also identified facilities-related decisions as a critical area. This document addresses both wired and wireless LAN and WAN services and provides commentary in the area of facilities planning.

In general, the document provides guidance and information to executive branch agencies in the following ways:

- Overviews of three technical topics: LAN, WAN, and facilities-related issues.
- Recommendations that agencies deploy technologies rated as "Strategic." This advice is presented in Tables within each Technical Topic. See tables in Technical Topics #1, **Local Area Networking** (LAN), page 11; #2 **Wide Area Networking** (WAN), page 14; and #3, **Facilities,** page 16.
- Recommendations that agencies follow proposed and existing **Information Technology Resource Management** (ITRM) **Policies, Standards, Guidelines** (PSGs). [1] The proposed policies, standards and best practices offered in this document will be reviewed by appropriate stakeholders and then converted into official ITRM PSGs. The policies, standards and best practices begin on page 17.
- A Glossary of technical terms beginning on page 24.
- Web links for more information provided for selected technologies are provided in the glossary.
- A brief paper on wireless networking is provided in Appendix C.

For LANs, the general approach recommended is use of Ethernet coupled with the bandwidth enhancement alternatives generally available in the marketplace. For WANs, the services presently available through the COVANET contract are detailed along with several other options for meeting bandwidth and connectivity needs. For wireless solutions, strong business reasons (e.g., mobility or historic preservation requirements) are recommended as an initial benefit argument to offset costs and operational problems.

[1] Some IT policies come about as a result of laws written by the General Assembly or Executive Orders written by the Governor's office; other IT policies are ITRM policies, standards and guidelines, which are developed by the Department of Technology Planning for the Secretary of Technology.

The cabled infrastructure has a longevity benefit that must be considered when comparing wired and wireless solutions and changing protocols. TCP and IP are the protocols recommended as a Client standard for moving data between desktopsand servers and to the Internet. Facility improvements that benefit premises infrastructure and its management are strongly encouraged.

Network Domain Team Mission

To define a network model as a foundation for meeting the present and future business communications needs of the Client.

Background

Client's **Enterprise Architecture**[2] (EA) includes business, governance and technical components that describe how Client will use technology and proven practices to improve the way it does business. Jointly, the technical components are referred to as the **Enterprise-Wide Technical Architecture** (EWTA). EWTA is comprised of eight domains. EWTA constitutes a comprehensive framework for providing technical guidance and related best practices to Client's agencies.

The EWTA is being developed in stages and will be updated routinely (see Figure 1 and Appendix A.). The **Council on Technology Services** (COTS) and its work groups are responsible for the development and updating efforts. Those involved began their efforts by specifying business strategies and information requirements, which were used to determine expectations for Client's future enterprise architecture. The following diagram summarizes the development process and identifies the responsible groups.

Figure 1: Development of the Enterprise-Wide Technical Architecture (EWTA)

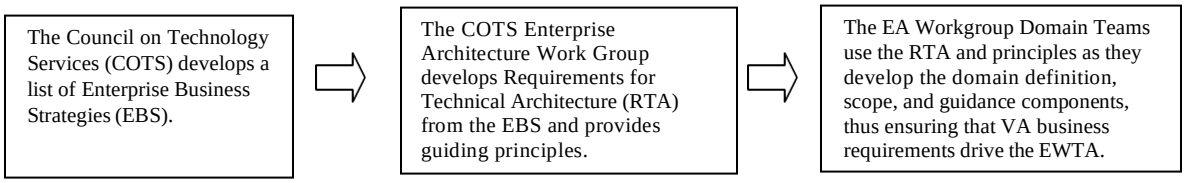


Table 1: EWTA Domains

Base	Functional Glue	Application
Network Architecture	Middleware Architecture	Systems Management Architecture
Platform Architecture		Database Architecture
		Application Architecture
		Information Architecture
Security Architecture		

The eight technical architecture domains are listed in Table 1. Each of the eight domains is a critical piece of the overall architecture. The Network and Platform Domains address

[2] Bold face type will be used throughout this document to indicate the definition of an acronym.

the infrastructure base. These two areas provide the foundation of any distributed computing architecture. Systems Management, Database, Application, and Information Domains provide vehicles for discussing the business functionality and management of the technical architecture. The Middleware Domain addresses the interfacing of disparate platforms, systems, databases and applications in a distributed environment. The final domain is the Security Domain, which addresses the many vehicles for enhancing information security across the architecture. These eight domains provide a useful way of communicating guidelines, policies, standards and best practices of the EWTA to stakeholders in state and local government agencies and state universities.

This document addresses only the Network Architecture, which is a base component of the EWTA. The document provides guidance regarding connectivity components (e.g., services and protocols used), defines obsolescent, transitional, strategic, and emerging directions for the components, and recommends policies, standards and best practices. The audiences for the resulting *Network Domain Architecture* document are the business and technical leaders in state and local agencies (universities, colleges, and agencies from all branches of government). This information will assist those who make technical decisions related to the communications and connectivity in being responsive to changing business needs in areas including bandwidth, quality-of-service, and mobility.

The terms "Obsolescent, Transitional, Strategic, and Emerging" as defined below will provide guidance regarding specific technologies throughout the document.

- **Obsolescent-**The Client Enterprise Architecture actively promotes that agencies employ a different technology. Agencies should not plan new deployments of this technology. Agencies should develop a plan to replace this technology. This technology may be waning in use or no longer supported.
- **Transitional**- The Client Enterprise Architecture promotes other standard technologies. Agencies may be using this technology as a transitional strategy in movement to a strategic technology. This technology may be waning in use or no longer supported.
- **Strategic**-The Client Enterprise Architecture promotes use of this technologyby agencies. New deployments of this technology are recommended**.**
- **Emerging**-The Client Enterprise Architecture promotes only evaluative deployments of this technology. This technology may be in development or may require evaluation in government and university settings.

In general, the document provides guidance and information to agencies in the following ways:

- Overviews of three technical topics: LAN, WAN, and facilities-related issues.
- Recommendations that agencies deploy technologies rated as "Strategic." This advice is presented in Tables within each Technical Topic. See tables in Technical Topics #1, **Local Area Networking** (LAN), page 11; #2 **Wide Area Networking** (WAN), page 14; and #3, **Facilities,** page 16.
- Recommendations that agencies follow proposed and existing **Information Technology Resource Management** (ITRM) **Policies, Standards, Guidelines**

(PSGs). [3] The proposed policies, standards and best practices offered in this document will be reviewed by appropriate stakeholders and then converted into official ITRM PSGs. The policies, standards and best practices begin on page 17.

- A Glossary of technical terms beginning on page 24.
- Web links for more information provided for selected technologies are provided in the glossary.
- A brief paper on wireless networking is provided in Appendix C.

The term "agency" means Client of executive branch agencies andinstitutions of higher education. For the purpose of this document, however, any academic "instruction or research" systems/infrastructure that can be isolated from "administrative and business" systems/infrastructure are considered exempt from thestated architecture standards.

Concerning local governments and other public bodies, while they are not required to comply with the standards, the information technology specifications for participation in state programs would be based on the architecture described herein. This architecture was designed with participation of local government and other public body representatives with the intent of encouraging its use in state/local interoperability activities.

Methodology

The network domain team began its work by defining network architecture, and by delineating the team's goals, objectives, and scope of work. Discussions included how the network domain interfaces with other architecture domains, the present and future directions for networking, and how often the information provided in this guideline would be updated. The team also reviewed input from publications and input from individuals with specialized knowledge. The results of the team's efforts and deliberations are provided throughout this document.

Network Architecture Definition

The network architecture defines a communications infrastructure model for the Client. It defines the various technologies required to enable connectionsamong governments and their citizen and business sector constituents.

Objectives

The network architecture addresses the networking requirements implied by the Client's business strategies. The Department of Technology Planning will ensure that domain team guidelines, best practices, and recommended standards includedin this document will be reviewed and revised routinely to provide up-to-date informationthat agencies can rely upon as they plan for their future connectivity and communicationsneeds.

[3] Some IT policies come about as a result of laws written by the General Assembly or Executive Orders written by the Governor's office; other IT policies are ITRM policies, standards and guidelines, which are developed by the Department of Technology Planning for the Secretary of Technology.

The domain team has addressed the following objectives in its initial work and will continue to do so during periodic reviews.

1. Provide guidance to agencies with the following goals in mind:
    a. encourage acquisition patterns within and across agencies that will result in economies of scale;
    b. promote simplicity across network solutions;
    c. promote interoperability (e.g., sharing information) among networked services;
    d. provide a long-term vision with opportunities for short-term payoffs;
    e. enable the "leveraging of network infrastructure investments" by business users rather than the "saving of money;"
    f. expand citizen/customer services by improving infrastructure functionality in the Client;
    g. improve decision making (through improved information flow) for all Client network users;
    h. help with technical decision making at the agency and Clientlevels;
    i. maximize portability across service providers;
    j. influence standards selection and development in areas such as wireless, where standards are evolving; and
    k. enable the convergence of voice, video, image and data services in the Client.
2. Recommend a framework of policies and standards to COTS.
3. Recommend best practices for the Client.

Network Architecture Components

Information in this guideline is presented for each of three domain components or technical divisions: Local Area Networking, Wide Area Networking, and Facilities Issues. Information is restricted to services, technologies, and environmental issues related to the first four layers of the **Open Systems Interconnect** (OSI) seven layer model of client to server communications (see Appendix B). Briefly, these layers include standards for the development of the 1) physical layer, 2) data link layer, 3) network layer, and 4) transport layer.

Whenever an important issue is noted that is outside of the scope of this document, the reader will be referred to another architectural domain document for clarification or detailed explanations.

In the past, control, ownership, and distance were defining dimensions that distinguished LANs from WANs. These lines are now beginning to blur and in the future, may blur even further. Application service providers, remote network managers, remote server

farms, wireless technologies, and mobile nodes contribute to this blur. Regardless, this local and wide area networking division provides a familiar structure for describing the present network architecture and how it will change as we move to the future.

Local Area Network Definition

A local area network is generally a private network. It is under the control of the owner and used by a set of related individuals and/or workgroups, typically within a single building or over a group of neighboring buildings.

Wide Area Network Definition

A wide area network connects local area networks to one another, generally using public infrastructure or services. The connections are made using the shared public infrastructure, public infrastructure leased for private use, and sometimes, private infrastructure (e.g., fiber) with public services.

Facilities Issues Defined

Facilities related issues are an important part of providing networks and should not be left to happenstance in the environments of the future. When networks were first introduced into agencies, each agency grappled with retrofitting problems and make-do answers. Now, as the Client moves forward, decision makers must ensure that future building leases, building renovations and construction activities address IT infrastructureneeds as a core need. Some technology-related building needs are beyond the network domain, but others are clearly critical to ensuring connectivity and communications.

Principles

Principles are guiding beliefs. They are intended as guidance for the domain teams. They are less specific than best practices, which are intended to guide agency decisions.

General Networking Principles

- The network architecture should be based on a set of standards that will enhance the availability of network support and provide a foundation upon which support planning can take place.
- Standardization on layered protocols provides user transparency.
- The network architecture should be based on a set of standards that will support the use of networks for integrated voice, video, image and data transmission.
- The Client must actively work on enabling the convergence of voice with data traffic over LANs and WANs. This convergence will require a **quality of service** (QoS) level approaching that provided by the existing **Public Switched Telephone Network** (PSTN).
- The Client should seek to meet a QoS guarantee within its network architecture.
- The key to ensuring affordable interoperability among domains is the promulgation of standards, and the adoption of these standards.

LAN Principles

- LAN design should be security neutral. LANs are designed for business connection and throughput needs, and should neither implement nor thwart security.
- Future LANs must provide mechanisms for addressing QoS.

WAN Principle

- The Client should ensure that contracts for WAN services offer flat ratepricing and require full geographic coverage to ensure geographic equity for localgovernments (implemented in 2000 COVANET contract).

Facilities Principle

- Telecommunications infrastructure planning is an integral part of facilities planning, leasing, maintenance, construction, and renovation.

Network Domain Components

In this section, LAN and WAN component technologies will be rated. As mentioned previously, the rating scheme is "Obsolescent, Transitional, Strategic, and Emerging."

Technical Topic #1: Local Area Networks

In the late 1980's to middle 1990's, state agencies were installing their first local area network services. Ethernet (10BaseT, star wired to hubs) emerged as the most widely employed solution. Today many agencies are replacing, reconfiguring, or upgrading their LANs to:

- expand existing services;
- redesign services due to relocation;
- improve throughput, availability or reliability of services; or
- accommodate a new mix of applications.

To provide guidance appropriate to these business needs in state and local agencies, this report will focus on the most widely employed LAN solutions and options for improving them. The network domain team views services not mentioned here as being in the Obsolescent category. Table 2 provides an overview of LAN services.

Table 2: Technology Use Trends for Wired LANs

Obsolescent	Transitional	Strategic	Emerging
Token Ring Appletalk	Ethernet 10Mbps ATM 25 Mbps	Ethernet 10/100Mbps Ethernet 100 Mbps Full Duplex yielding up to 200Mbps EtherChannel 200 to 800 Mbps Gigabit Ethernet backbone	Gigabit Ethernet LAN

The vast majority of state and local agencies are presently supporting mixed 10Mbps and 100 Mbps Ethernet services (strategic). Network administrators are buying 10/100 Mbps

capable **Network Interface Cards** (NICs) in new equipment and are replacing old hubs with switches as they slowly transition to totally switched environments. Most agencies have a mix of old and new equipment attached to their LANs. The older equipment may have 10 Mbps NICs and may not be upgradeable (e.g., no available Peripheral Component Interconnect (PCI) slots). The transition from Fast Ethernet (100 Mbps) performance to Gigabit Ethernet performance is not a single discrete step, but a continuum. Use of switched full duplex links can bring performance of a single connection to as much as 200 Mbps, depending on traffic symmetry. Use of **EtherChannel** (aggregation of multiple physical Ethernet links into a single logical link) can result in throughputs of up to 800 Mbps on server connections and **Inter-Switch Links** (ISLs). Since most switch backplanes exceed a gigabit (1.2 to 4 Gbps service is common on low- to mid-range switches), these methods can often be used to approach Gigabit Ethernet speeds while using Fast Ethernet components.

Presently, few business applications demand the still expensive gigabit Ethernet services. Gigabit Ethernet service to the desktop is viewed by the team as emerging because, even though it is a viable alternative, it is rarely employed due to cost. Some agencies may employ gigabit Ethernet as a backbone technology and this use is listed as strategic.

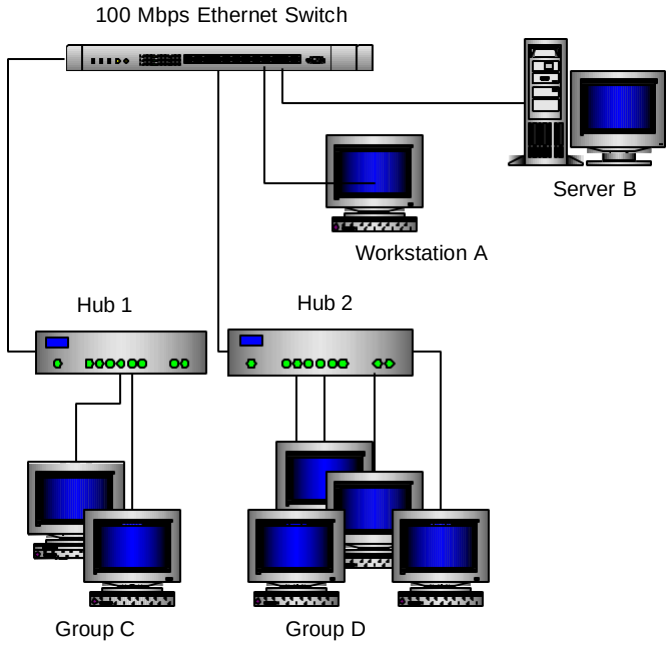
Token Ring, although a stable technology with its own upgrade path for greater bandwidth, is listed as Obsolescent. The main reason for this classification is shrinking market share. Token ring implementations continue to dwindle. Ethernet is the replacement technology of choice. In Client government, there are several existing usesof Token Ring. Token ring has not been replaced in these instances because Token Ring layer 2 addresses (i.e., **Media Access Control** (MAC) addresses) are used in providing terminal emulation for important mainframe applications. In these situations, the application layer code is dependent on Token ring layer two addresses.

Table 3: LAN Technologies

Service (Bandwidth)	Typical Deployment	Data Link/ MAC	Network/ Transport
Token Ring IEEE 802.5 (2-16 Mbps; 100Mbps solutions available)	**Category 5 Unshielded twisted pair** (Cat 5 UTP); 16 Mbps NICs; hubs (switches may be used but the network then functions more like switched Ethernet than Token Ring)	Token passing ring	**IP** (Internet Protocol) addressing and TCP (Transmission Control Protocol) recommended in this document as standard for the Client
Ethernet IEEE[4] 802.3 (10 Mb)	Cat 5 UTP; 10Mbps and 10/100 NICs; hubs and/or switches	**CSMA -CD**[5] with collisions reduced by switching and segmentation.	
Asynchronous Transfer Mode (ATM) LAN (25 Mb)	Cat 5 UTP; ATM NICs. Use is extremely rare.	Emulation of Ethernet	

Service (Bandwidth)	Typical Deployment	Data Link/ MAC	Network/ Transport
Fast Ethernet, **Full-duplex Fast Ethernet, and** **Fast EtherChannel** IEEE 802.3[6] (10/100Mb)	Cat 5 UTP; Switched 10 and 100 Mbps segments with 10/100 NICs; switches cascading to hubs. Speeds over 100 Mbps are rarely deployed at present. ISL is available on Catalyst switches and Cisco routers. Multi-port NICs are used.	CSMA-CD with collisions reduced by switching	Other protocols in common use include **IPX/SPX** (Netware layers 3 and 4 protocols)
Gigabit Ethernet IEEE 802.3z (1000 Mbps)	Gigabit NICs; Switches; Cat 5e. To the desktop is possible but expensive; backbone use is more prevalent. Cat 5e, switches; fiber backbones	CSMA-CD with collisions reduced by switching	

Figure 2. Switched Fast Ethernet LAN Configuration Example



- 100 Mbps switched service to each of 4 LAN segments.
- Server A sends to Workstation B at 100 Mbps dedicated bandwidth
- Group C Workstations share 100 Mbps service (cascading hub).
- Group D Workstations share 100 Mbps service (cascading hub).

[4] Institute of Electrical and Electronics Engineers (a standards group)

[5] Carrier Sense Multiple Access with Collision Detection (the method by which Ethernet users' packets access shared media)

[6] EtherChannel is a proprietary Cisco solution. Cisco states: "Cisco's Fast EtherChannel technology builds upon standards based 802.3 full duplex Fast Ethernet to provide network managers a reliable high speed solution for the campus network backbone. Fast EtherChannel provides bandwidth scalability within the campus by providing increments from 200 Mbps to 800 Mbps with multi-gigabit capacity in the future. Fast EtherChannel technology not only solves the immediate problem of scaling bandwidth within the network backbone today, but also paves the path for an evolution to standards-based Gigabit Ethernet and beyond, because Fast EtherChannel technology can be applied to support Gigabit EtherChannel."

The main factors making wireless LAN solutions less attractive are higher costs, lower bandwidth, and variable signal quality (environmental effects). Deployments of wireless LANs or WANs should include a thorough testing of the environment.[7]

Table 4: Technology Use Trends for Wireless LANs

Obsolescent	Transitional	Strategic	Emerging
	Infrared (Point to Point, IEEE 802.11)	**Frequency Hopping Spread Spectrum** (FHSS, IEEE 802.11)	
		Direct Sequence Spread Spectrum (DSSS, IEEE 802.11 and 802.11b)	

Technical Topic #2: Wide Area Networking

For WAN services, state agencies are required by law to use contracts negotiated by DIT. The services listed in Table 4 below are those services presently available as part of the contract known as COVANET. Because the COVANET contract offers flat rates (same rate regardless of location) and month-to-month contracts, it affords state and local government agencies considerable opportunity for flexibility and scalability; however, substantial lead time is required to effect the initiation of certain service (e.g., 6 weeks to 6 months lead time may be required depending on the service, the provider, the geographic location, and agency facilities). Delivery of the local loop may be the slowest link in obtaining new wide area service.

Table 5 indicates the service name, medium and bandwidth ranges for available WAN services. With the exception of **Digital Subscriber Line** (DSL), all services may be requested by all localities. DSL services are available only for uses within 18,000 feet or about 3.5 miles of a **Local Exchange Carrier Central Office** (LEC CO). These distances can be extended by the use of repeaters. Lead-time requirements for service provision will be longest in those localities with low population densities. A six to twelve month advanced notice to the Department of Information Technology (DIT) will help to ensure service availability at the time it is needed.

As COVANET is a relatively new contract (June, 2000), services offered are mainly rated as strategic. Some explanation is required for those services listed as Transitional or Emerging. 56 Kbps Frame Relay and 64-128 Kbps **Integrated Services Digital Network** (ISDN) are listed as Transitional because they are low-bandwidth solutions and relatively costly. The team believes that these services will not be available in the long run. xDSL services (i.e., various digital subscriber line services including ADSL (**asymmetric DSL**) and others), on the other hand, have recently shown uncertain market support. Due to market support problems they are placed in the Emerging category. Cable modem services have been used in school settings and are gaining in popularity in the home market, but have not been used widely for business purposes.

[7] Note: Running 802.11b technologies and Bluetooth in the same environment results in interference. The degree of susceptibility to interference increases in proportion to the strength of the DSSS signal and the distance between the 802.11b access point and the wireless client. See LAN standards do battle, J. Wexler.

Table 5: Technology Use Trends for Cabled Wide Area Networking

Obsolescent	Transitional	Strategic	Emerging
	Frame Relay 56 Kbps	Dialup (28.8-56 Kbps)	xDSL (128 Kbps—8 Mbps)
	ISDN—narrow band (64—128 Kbps)	Frame Relay T1 (128 Kbps-1.5 Mbps)	Cable Modem (300 Kbps—10 Mbps)
		ATM T1 (1.5 Mbps)	
		Aggregated Frame Relay, i.e., 2, 3, or 4 T1s (3-6 Mbps)	
		Frame Relay DS3 (22 or 44 Mbps)	
		ATM DS3 (22-45 Mbps)	
		ATM SONET (synchronous optical network) over OC3 (optical carrier) to OC12 (155-622+ Mbps)	

Some may wonder why dial up connections are in the "Strategic" category. Dial up connections continue to be widely used by traveling state workers, telecommuters, university students, small agencies, network support staff for remote server connections, and out-of-band vehicles. For citizens, it is still the most common method for obtaining Internet connectivity.

Local governments, colleges, and school divisions often install their own dark fiber cables or leverage cable TV and other telecommunications contracts to acquire and install dark fiber that will be owned by the government. In Canada, dark fiber may be installed on behalf of a consortium with schools or other groups owning strands (condominium fiber). A typical government use of the dark fiber is the creation of campus LANs or metropolitan area networks (MANs or metro WANs). Having privately-owned dark fiber provides a certain level of control over future telecommunications costs. The owner has many choices for lighting the fiber connections between buildings ranging from internal provision of fast Ethernet (100 Mbps) or Gigabit Ethernet LAN services to internal or external provision of WAN services. The owner is able to level the playing field between WAN service providers that own infrastructure and those who do not, thus increasing competition and reducing costs. Also, as bandwidth needs increase, those localities that contract for externally provided services have the option of more easily switching to higher bandwidth services such as dense wave division multiplexing (DWDM). (See FAQs at http://www.canet3.net for additional information on this topic.)

Wireless WAN services are used to provide connectivity for mobile user. In Europe, radio frequency based services are standardized (***Groupe Speciale Mobile*** or GSM). In the United States, a variety of proprietary standards are employed.

Wireless services are presently not available on the COVANET contract. Most wireless services listed in Table 6 are rated Strategic. Considerable information from the O'Reilly dictionary (http://www.oreilly.com/reference/dictionary/tsearch.cgi) is presented for each of the wireless protocols and services in the Glossary. Links to these definitions are

provided in Table 6. Also, see the footnotes for some of the less well-known technologies in Table 6. Additional information on wireless technologies and services may be accessed at http://www.mobileinfo.com/Product_Dir/products_infra.htm and in Appendix C.

For all WAN services, agencies should contact a DIT COVANET representative to discuss business requirements for bandwidth and QoS. WAN services will continue to evolve as bandwidth in the LAN environment increases towards gigabit service. According to GartnerGroup, the cost of providing high bandwidth WAN and LAN services will drop so considerably that "throwing bandwidth at the problem" will become a design principle. GartnerGroup also notes that some WAN premises equipment will migrate to the service provider side of the equation, leaving WAN managers to manage services and not equipment.

Table 6: Technology Use Trends for Wireless Wide Area Networking

Obsolescent	Transitional	Strategic	Emerging
	ARDIS[8](9.6—19.6 Kbps)	Cellular[9], CDMA (9.6—19.6 Kbps)	Broadband PCS[10], limited speed and limited graphics (56 Kbps)
	Satellite, high cost, (56 Kbps)	Circuit/Packet Data, CDPD; service area restricted to population crescent (9.6—19.6 Kbps)	CDMA 2000, proposed 3rd generation standard (144 Kbps)
		Frequency Hopping Spread Spectrum, FHSS (2 Mbps)	
		Direct Sequence Spread Spectrum, DSSS (2—11 Mbps)	
		Mobitex or RAM Mobile Data[11]; uses MASC protocol and has a limited service area (9.6—19.6 Kbps)	
		Microwave –this privately owned strategy is generally as expensive as trenching, but may be less expensive than associated right-of-way acquisition.	
		Infrared Point to Point solution for backbone up to 2.46 mi. OC12 throughput	

[8] ARDIS is a public data communications wireless network for handheld devices to send/receive short data messages. One example use is the sheriff on the street searching a department database for unpaid tickets. ARDIS is jointly owned by IBM and Motorola.

[9] Cellular services are those spread-spectrum digital wireless service that supports voice and data transmission. They use one of three access technologies, **Code Division Multiple Access** (CDMA), **Time Division Multiple Access** (TDMA), or **Frequency Division Multiple Access** (FDMA). Cellular services operate at 800 MHz.

[10] PCS is Sprint's **Personal Communications Services**. It operates in the 1.9 MHz band. It is not a cellular service. (600mhz, 900mhz).

[11] Mobitex, RAM or RAM Mobile Data. Presently owned by Bell South. (A competitor of ARDIS).

Technical Topic #3: Facilities and Related Considerations

Facilities play an integral part in the selection and deployment of LAN and WAN services. Considerations including geographic location, line-of sight, and distance from the LEC CO may affect WAN choices. The unavailability of suitable wiring closet space may add to maintenance and replacement costs due to dirt, foot traffic, physical security, equipment inaccessibility, and other problems. Although it may not always be possible to follow the best procedure, agencies are encouraged to estimate the costs associated with the less preferred alternative (i.e., using whatever space is available) when putting forth cost-benefit arguments for such activities as building a secure, climate-controlled wiring closet, acquiring equipment enclosures, or other facilities-related improvements. Several best practices regarding facilities are provided in the next section.

Policies, Standards and Best Practices

The domain team has developed several recommendations, which are presented in this section. Policies are high-level requirements for agencies. An example would be a requirement that all agencies have a security policy. Standards are existing standards (e.g., **Council on Information Management** or CIM Standards) that the domain team recommends to be continued and/or updated and continued. Recommended Standards are recommendations awaiting COTS approval. Standards are mandatory requirements. Best practices are intended as guidance. Agencies should consider the following Recommended Standards and Best Practices when designing and implementing network services or service enhancements.

Policies

Policy 1. *State Agency Telecommunications Contracts.* Current law states all voice and data telecommmunication services (e.g., WAN services) for state agencies must be provided by DIT or exceptions approved by DIT. (See *The Code of Client*, § 2.1-563.17, Powers and duties.) Local agencies and other public bodies are encouraged to take advantage of these contracts.

Policy 2. *Telecommunications Acquisitions by State Agencies.* Current law states that information technology acquisitions over $100,000 must be approved by the Department of Technology Planning and acquisitions over $1,000,000 must be approved by the Secretary of Technology. (See *The Code of Client*, § 2.1-51.47 B.6., Powers and duties.)

Recommended Policies

Recommended Policy 1. *State Facilities.* Public and private network infrastructure requirements must be an integral part of building design, leasing, construction and renovation and should be appropriately scheduled to ensure service availability. This practice will help agencies to avoid time delays and future inflated expenses.

Recommended Policy 2. *State and Local Agency IP Addresses.* State and local agencies sometimes route unregistered IPv4 addressed packets (i.e., RFC 1918) over COVANET. Any state or local agency intending to do so must first gain DIT approval and record the unregistered address range they are using with DIT. State

and local government agencies are strongly encouraged to employ only registered IPv4 addresses when routing over COVANET and are required to use only registered IPv6 addresses when they switch to IPv6. (A **Freedom of Information Act** (FOIA) exception[12] to the sharing of DIT recorded IP address information would be sought prior to implementing this policy).

Standards

- *Telecommunications Cabling (ITRM 95-1) The e*xisting Client standard for telecommunications cabling references ANSI EIA/TIA[13] cablingstandard as follows: cabling, 568 A/B; pathways and spaces, 569; building wiring, 570; grouping and bonding, 607; and administration, 606. (See modification recommendations below.)

Recommended Standards

Recommended Standard 1. *Telecommunications Cabling (ITRM 95-1)* The existing Client standard for telecommunications cabling references ANSI EIA/TIA cabling standard as follows: cabling, 568 A./B.; pathways and spaces, 569; building wiring, 570; grouping and bonding, 607; and administration,606. These standards are recommended for continuation as standards with updates through the latest EIA/TIA addenda being required unless exceptions are specifically noted.[14] Clarifications are needed as follows:

- Clarify and update wording of the existing standard. One example would be clarification of the two jack minimum requirement. This requirement is for a minimum of two jacks at each cable termination location. In addition, contracts for new cabling plants must meet the following minimum standards.
- Category 5e cabling with certification testing using Level IIE field testers is the recommended minimum standard for all new or replacement installations of a horizontal medium for wired LANs in the Client. Addendum 5to EIA/TIA 568A specifies the Category 5e implementation. Tested category5e cabling and parts enable a consistent upward migration path for agencies, ensure high bandwidth transmission capabilities over copper, and provide progress towards a viable gigabit connection to meet future needs.[15]

[12] DTP should request that the Secretary of Technology encourage the sponsoring of legis lation to grant the needed Freedom of Information Act (FOIA) exception for centralized IP address information for security reasons.

[13] American National Standards Institute has certified that the Electronic Industries Association and Telecommunications Industry Association have used appropriate methods to arrive at a standard.

[14] A revised telecommunications cabling standard (i.e., replacement for Client of Client (COV) ITRM Standard 96-1)will be issued by July 1, 2001 by DTP.

[15] Category 6 cabling standard, EIA/TIA 854 is anticipated in mid 2001. Category 7 standards are expected mid year also. At this point in time, complete standards are available only for Category 5e as an addendum (5) to EIA/TIA 568A. Presently available Category six implementations are based on proprietary protocols. The costs and benefits of Category 6 versus Category 5e cannot be determined at this time.

- A 25 year warranty of certification test results. When state agencies contract for cabling, the contract must include testing and provide a 25 year warranty. Contractors typically address such a warranty by providing a tested, same-vendor installations (same-vendor parts) to ensure the 25-year availability of service. State agencies that provide their own cabling or testing are not required to provide this certification.

Recommended Standard 2. *Network Addressing and Transport Protocols* IP is the standard network addressing protocol and TCP, the standard transport protocol for the Client. Agencies are to develop plans for ensuring all LAN nodes and LAN segments may be accessed using IP addressing no later than December of 2003. When other protocols are essential, agencies should encapsulate the protocol within TCP/IP for external routing. All external connections to state agencies and local governments (e.g., vendors, business partners, contractors, and the public) should be made using TCP/IP protocols. Useof obsolescent, proprietary OSI Model layers 3 and 4 protocols such as AppleTalk, SPX/IPX, and LAT is discouraged unless necessary as a legacy transition strategy. Local agencies are encouraged to migrate away from these protocols as well.

Recommended Standard 3. *Standard LAN*. 100BaseT Switched Ethernet is the minimum LAN service recommended for new acquisitions by state agencies. All switches should be 10/100 Mbps capable if needed to allow the servicing of older 10 Mbps interfaces. To support QoS, the switch needs to be a "managed" switch. Local agencies are encouraged to use the above standard as a cost-effective method of increasing LAN bandwidth whenever bandwidth contention on a 10 Mbps Ethernet network is observed (sustained usage at or above 50%).

Recommended Standard 4. *Device Management.* All managed network devices acquired by state agencies must be **Simple Network Management Protocol** or SNMP manageable.[16] Local agencies are encouraged to use SNMP as a management unifying approach as well.

Recommended Standard 5. *Cabling* . Cabling, electrical and other facilities work done by state agencies must comply with appropriate building codes. Local agencies are encouraged to comply with building codes to reap safety, security, and management benefits.

Best Practices

Best Practice 1. *State and Local Agency Interconnections for Telecommunications.* If state and local agencies need to communicate with one another, COVANET is strongly recommended as a cost-effective vehicle that should be used (i.e., for new contracts). Agencies are responsible for providing the gateway between their network and COVANET. Universities may have alternate university to university connections for distance education or research (e.g., Internet 2) that should be leveraged rather than using COVANET.

[16] For additional information on the Simple Network Management Protocol, see Middleware Domain Guidelines.

Best Practice 2. *Network Planning and Application Changes*. State and local agencies should ensure that network planning is well integrated with applications design/acquisition and roll out. From the application analysis stage through the design/acquisition stage, agencies should review application bandwidth requirements, real-time data flow needs, and expected system capacity changes from other sources. These reviews should be conducted quarterly.

Best Practice 3. *Strategic Planning.* State and local agency heads should review business changes with networking staff or network providers to ensure network implications are addressed in a timely manner. Changes in business volume, staffing levels, applications, or facilities (e.g., relocation, construction, or renovations) may affect network services.

Best Practice 4. *Telecommunications Service Change Planning.* State and local agency telecommunications planners should confer with the Department of Information Technology (DIT) regarding the amount of lead-time required to make service changes involving DIT telecommunications contracts. (DIT holds Telecommunications contracts for state agencies in the Client as provided in the *Code of Client*, § 2.1-563.17. Powers and duties).

Best Practice 5. ***Domain Name Systems*** *(DNS).* State and local agencies should have a primary and a secondary DNS (required for domain registration), each of which should reside on a separate network. This practice enables the agency Web site to remain visible to users if one network is down. DIT provides a secondary DNS for COVANET customers. [17]

Best Practice 6. *Planning for Voice, Video and Data.* When designing new networks, state and local agencies should design for voice, video, data, and image traffic on the network. Although Gigabit Ethernet is rarely provided to the desktop, it is in common use as a backbone technology and should be considered. Examples of other design components to address potential future business needs are layer three intelligent switches, layer 4 bandwidth management facilities, and switched 100 Mbps Ethernet service. No known agency application would warrant Gigabit Ethernet to the desktop.

Best Practice 7. *Network Planning and Risk.* State and local agencies should allow security and risk planning decisions to drive decisions regarding network design for redundancy, fail-over, and disaster recovery.

Best Practice 8. *Wireless LANs.* State and local agencies should implement wireless LANs only when they have good business reasons to implement them and cost/benefit justifications. Future change requirements should be considered. (See issues in Appendix C.)

Best Practice 9. *Wireless Services*. State and local agencies deploying wireless LAN/WAN services should conduct thorough site survey including testing/inspection.

[17] See Middleware Guidelines for additional discussion of DNS.

Best Practice 10. *Test Environment.* When adding new applications to a network, state and local agencies should establish a test environment (platform). Agencies should use a parallel network infrastructure (in-house environment or vendor provided environment). The test environment should not exceed the requirements of the planned operational environment. An alternative to a test environment would be use of a controlled, measured implementation (validates network needs above). Whenever possible, the development environment should model and not exceed the infrastructure of the planned operational network environment (e.g., available bandwidth).

Best Practice 11. *LAN Bandwidth Management*

- *(Switches)*. Network administrators serving state and local agencies should convert central hubs to switches to realize an instant performance increase and to enable better management of bandwidth, even in a 10 Mbps Ethernet or a Token Ring environment. Switches operate at layer 2 in the manner of multiple bridges and vastly reduce collisions and thus, the need for repeat traffic. The old hub can be connected to the switch to cascade bandwidth to low-end users.
- *(Bottlenecks)*. Network administrators should identify the bottlenecks respons ible for throughput degradation and attempt to address them. Workstations, RAIDs, and servers can be involved. Just upgrading from 10 Mbps to 100 Mbps Ethernet service may not fix a workstation or server I/O problem. If equipment is old, it may not have a PCI slot for a 10/100 NIC.
- *(Re-segmenting).* Network administrators should consider re-segmenting a LAN segment and when sustained usage exceeds 50% on a regular basis.
- *(Routers).* Routers are slow and can be the cause of a bottleneck. Network administrators should replace internal routers with layer 3 switches to achieve a performance boost.

Best Practice 12. *WAN Bandwidth Management.* Whenever WAN bandwidth usage is sustained at 50% or higher or future usage is forecast at 50% or higher, network administrators should determine the causes and attempt to alleviate the contention. If unable to reduce the contention through means such as rescheduling, the network administrator should consider increasing bandwidth.

Best Practice 13. *New Technologies.* The Client should put into place a mechanism for monitoring new, key LAN and WAN services and technologies. When they are fully accepted, viable, available, and supportable, this informationshould be conveyed to **Agency Information Officers** (AIOs) and other decisionmakers. The domain team should ensure the information is integrated into the *Networking Architecture*. DTP is recommended as the coordinating agency.

Best Practice 14. *Single Pipeline.* If all federal security and cost issues could be resolved and if all state and local governments would use COVANET, single pipeline efficiencies in costs and management could be realized. The following current problems would be addressed.

- Local service branches of state agencies often must support multiple connections to state and county/or city government offices.
- Local governments often must support connections to multiple state agencies and local agencies.
- State agencies must often support connections to multiple local agencies and to multiple state agencies.

The COTS **State and Local Network Integration Workgroup** (SLANI) proposed a single pipeline solution. The network domain team recommends that COTS support this concept by forming a workgroup to develop a strategy for addressing each of the barriers to the single pipeline. The strategy might, for example, include working with the federal agencies to obtain traffic mingling agreements and cost allocation method agreements.

Best Practice 15. *Expertise Pooling.* COTS should develop a mechanism for informal sharing of expertise across agencies, including DIT. An example would be technology topic meetings, user groups, or sharing of briefing papers from investigating technologies.

Best Practice 16. *Remote Deployment*. In situations where technical staffs are not locally available, state and local agencies should consider the management, maintenance and service issues associated with remote deployments.

Best Practice 17. *Electrical Service*. State and local agency network infrastructure addition and/or revision plans should include an analysis of the adequacy of electrical service. Also, agencies should provide adequate electrical outlets for application testing infrastructure.

Best Practice 18. *UPS* State and local agencies are strongly encouraged to use continuous inversion, **uninterruptible power supply** units (UPSs) with power conditioning. The UPS units should provide 15 minutes of battery backup for most network equipment and 30 minutes for servers. UPS units that automatically shut down in a controlled manner are preferred for servers.

Best Practice 19. *Wiring Closets*. State and local agencies should provide a secure, climate-controlled area for servers and networking components (e.g., switches, routers etc.). Agencies are encouraged to use racks or cabinets to maximize the utility of space available and to ensuring adequate space for easy access to the front and rear of network equipment and servers.

Beyond the Domain Scope

The list below directs readers to other domains of the enterprise architecture for topics related to networking but beyond the scope of the Network Domain.

- *SNMP* is an OSI layer 7 protocol that must be addressed to some extent in the network domain (e.g., RMON required on all OSI layer 1-4 devices to enable management). Additional discussion of SNMP may be found in the Middleware and Systems Management Domains.

- The network domain must touch on a number of *protocols that operate outside of the first four OSI layers including DNS, DHCP, LANE*, etc. Additional discussion of these protocols are found in Systems Management and Middleware Domains.
- Certain *management issues* critical to the proper operation and functioning of the network receive additio nal discussion in the Systems Management Domain. Issues related to the operation and management of distributed systems also belong in the Systems Management Domain.
- ***Virtual Private Networks*** or VPNs are discussed in the Security Domain.
- *Tunneling protocols* (e.g., for the purpose of routing for un-routable protocols) including Cisco layer 2 forwarding protocol (L2FP) are Network Domain protocols, but the purposes for which they are used are more appropriately discussed in the Security Domain (e.g., encapsulations of encrypted data, etc).
- Issues related to the *operation and management of network operating systems* are addressed in the Systems Management and Platform Domains.

Glossary

10BaseT- 10 Mbps Ethernet standard

100BaseT- 100 Mbps Fast Ethernet standard

ANSI - A voluntary non-profit organization that coordinates and supports the U.S. voluntary consensus standards for industry.

AIO- Agency Information Officer. VA law requires each agency to appoint an AIO.

ARDIS - A company that provides a cellular packet-switched radio data service in the U.S. Now completely owned by Motorola. (It used to be a joint venture with IBM.) Initially (1984), the network was designed by Motorola for IBM field service technicians. The radio protocol is proprietary (designed by IBM and Motorola). Has about 34,000 subscribers, about 10 times the number that RAM Mobile has. Data transmission is at 4,800 bits/s (using 240-byte packets, resulting in about 2,000 to 3,000 bits/s of user-data throughput) or 19,200 bits/s (in larger U.S. centers) using 512-byte packets, resulting in up to 8,000 bits/s of user-data throughput. Usage charges are per kbyte of data transferred. Sometimes called Datatac. Competes with RAM Mobile Data's Mobitex system and CDPD. Ardis is at http://www.ardis.com/ . (Taken from O'Reilly) Return to Table 6.

Asynchronous Transfer Mode (ATM) - 1. A cell switching technology that transports data at high speeds in small, uniform cells (packets). ATM may be used in LAN and WAN communications.

ATM/SONET - Asynchronous Transfer Mode cells carried over Synchronous Optical Network packets.

Backbone - A high-speed computer network designed to interconnect lower-speed networks or clusters of dispersed user devices.

Backplane- A backplane is an electronic circuit board containing circuitry and sockets into which additional electronic devices on other circuit boards or card can be plugged.

Bandwidth - The carrying capacity of a circuit, usually measured in bits per second for digital circuits or hertz for analog circuits.

Broadband Integrated Services Digital Network (B-ISDN) - A network technology that integrates interactive voice, data, and video by using cable TV's broadband channels. Uses Asynchronous Transfer Mode.

Cable Modem- A cable modem provides variable speed transmission depending on the number of simultaneous users on the same cable.

Cat 5e- Category 5e standard wiring

CCITT - 1. Consultative Committee for International Telegraph and Telephone. CCITT is a subagency of the United Nations. CCITT's three primary areas of investigation are data communications, telemetric services, and integrated services. CCITT is a division of the International Telecommunication Union (ITU).

CDMA- Code division multiple access. A form of multiplexing where the transmitter encodes the signal using a pseudo-random sequence which the receiver also knows and can use to decode the received signal. Each different random sequence corresponds to a different communication channel. Motorola uses CDMA for digital cellular phones. Qualcomm pioneered the introduction of CDMA into wireless telephone services. Return to Table 6.

CDMA 2000- code-division multiple access (CDMA) version of the IMT-2000 standard developed by the International Telecommunication Union (ITU). The CDMA2000 is third-generation (3-G) mobile wireless technology that can provide mobile data communications at speeds ranging from 144 Kbps to 2 Mbps. Deployment is in the planning stages. Return to Table 6.

CDPD- A wireless standard that provides two-way, 19.2 kbps packet data transmission over existing cellular telephone channels. A method proposed (1993) and developed by IBM and McCaw Cellular Communications, Inc. (now owned by AT&T) to more efficiently carry data on existing analog (AMPS) cellular radio systems. 138-byte packets of data are sent at 19,200 bits/s during gaps in conversations or on unused (no voice conversation established at that time) channels, using the full 30-kHz bandwidth

of the channel. Voice always has priority. Actual air traffic consists of blocks of 63 (47 are information, 16 are forward error correction information) six-bit symbols, resulting in a user data rate of about 9,000 to 14,400 bits/s. The forward error correction can correct up to eight six-bit symbol errors. Advantages over Ardis and Mobitex include the following: use of the existing cellular radio infrastructure (CDPD overlays it), resulting in lower usage charges; built-in encryption and authentication; the land-line interface is TCP/IP; security, since the data for a conversation are carried over many cellular radio channels (according to whichever has spare capacity), so it would be difficult to monitor the communication; V.42bis data compression; multicasting (to subsets of users); and a full-duplex option. Will be an open specification that will compete with the proprietary systems from Ardis and Mobitex (RAM). Is a packet-oriented service, so the call setup time is fast (much faster than circuit-switched), charging is by the kilobyte of traffic carried, and it is best-suited to smaller transactions (up to 5 Kbytes of data--larger transfers are better handled by circuit-switched methods, such as analog cellular with modems). Promoted by five of the seven U.S. RBOCs and Motorola, Microcom, and some cable TV companies. Return to Table 6.

CMSA CD- Carrier Sense Multiple Access with Collision Detection. An OSI level 2 media access method used by IEEE 802.3 Ethernet.

COVANET- is a comprehensive array of communications services - voice long distance, data, and Internet services to local and county governments, state agencies, universities, and quasi-government agencies.

COTS- Council on Technology Services. An advisory group for Client's Secretary of Technology

DIT – Client's Department of Information Technology (provides selected computing services).

DMV- Client's Department of Motor Vehicles.

DS3- A signal with a transmission rate of 44.736 Mbps (672 voice channels) provided over T3.

DSL- Digital Subscriber Line.

DSSS-Direct Sequence Spread Spectrum. A method of providing wireless connectivity as specified in IEEE 802.11b.

Emerging- A technology or protocol rating used in this document. Defined as "The Client Enterprise Architecture promotes only evaluative deployments of this technology. This technology may be in development or may require evaluation in government and university settings."

EMI- Electromagnetic interference.

Encapsulation - A technology where data and logic are protected from uncontrolled external access. Data is considered encapsulated if it can only be accessed via the software programs that manage it.

Ethernet - A local-area network (LAN) protocol that is specified in IEEE 802.3 and that uses CSMA-CD to provide 10 Mbps service over copper.

EWTA-The Enterprise Architecture has business and technical components. All of the technical components taken together are called the Enterprise Wide Technical Architecture.

Fast EtherChannel – A Cisco proprietary method for increasing bandwidth by aggregating ports. The following link provides Fast EtherChannel literature.
http://www.cisco.com/warp/public/cc/techno/media/lan/ether/channel/prodlit/index.shtml

FDMA- Frequency division multiple access.

FHSS-Frequency Hopping Spread Spectrum. A method of providing wireless connectivity as specified in IEEE 802.11.

Frame Relay - A data communications interface that provides high speed transmission with minimum delay and efficient use of bandwidth. It does not have error detection or error control and it assumes that connections are reliable.

GSM – 1. *Groupe Spéciale Mobile*—the European standards group for wireless connectivity. 2. Digital cellular telephone standard developed by the European Telecommunications Standards Institute's (ETSI)

Groupe Spécial Mobile . Also used in some Middle Eastern countries and parts of Australia. The frequencies allocated to the service are divided into 200-kHz blocks, each of which supports eight simultaneous users (by using a form of TDMA that lets a handset transmit a few bytes of data or digitized voice, 217 times per second).

Hub - 1. A LAN wiring concentrator that connects cables from numerous network devices. An intelligent hub can monitor and report on network activity, typically using SNMP.

IEEE- Institute of Electrical and Electronics Engineers, Inc. www.ieee.org

Infrared - Electromagnetic waves in the frequency range just below visible light corresponding to radiated heat.

I/O - Input/Output

Integrated Services Digital Network (ISDN) - A set of communications standards allowing a single wire or optical fiber to carry voice, digital network services and video

International Telecommunication Union (ITU) - an intergovernmental organization through which public and private organizations develop telecommunications.

Internet - 1. A wide area network connecting disparate networks world wide. 2. An international network of millions of web sites that uses TCP/IP.

Internet Assigned Numbers Authority (IANA) - An internet central registry for the assigned values of the addresses (in the form of numbers) used in TCP/IP network protocol implementations.

Internet Engineering Task Force (IETF) - A large, open, international community of network designers, operators, vendors, and researchers concerned with the evolution of the internet architecture and the smooth operation of the internet. IETF is generally recognized as the standards organization for the Internet.

Internet Protocol (IP) - A communication protocol which routes packets of data from one node on the internet to another. IPv4 routes each packet based on a 32 bit destination address called an IP address (e.g., 123.122.211.111).

IPv4-four octet 32 bit IP address in the form 255.255.255.255

IPv6- sixteen octet 128 bit IP address. For a discussion and comparison with IPv4 see NCS http://www.ncs.gov/n6/content/tibs/html/tib97_1/sec5_0.htm.

IPX - A network layer protocol initially developed at XEROX Corporation and made popular by Novell, Inc. as the basic protocol in its NetWare file server operating system.

ISDN - Integrated Services Digital Network.

ISL – Inter-switch links. ISL uses 100-Mbps Ethernet and allows the multiplexing of multiple VLANs over a single link.

ITRM – Information Technology Resource Management. A Client term used with policies, standards, guidelines and other management tools that are provided by the Department of Technology Planning for use by state and local agencies. E.g. ITRM Policy GOV2000.

L2FP- Layer 2 Forwarding Protocol, which was developed by CISCO supports the creation of secure virtual private dial-up networks over the Internet.

LAN- local area network.

Level II E Tester - Testing equipment used to certify Category 5e cable. A white paper on cable performance testing is provided at http://www.wirescope.com/whitepap/white24.htm.

Local Area Network (LAN) - 1. A private computer network generally on a user's premises and operated within a limited geographical area.

Local Exchange Carriers (LECs) - Local telephone companies: Southern Bell, GTE, and Sprint. Often, CLECs or competitive local exchange carriers.

MAC address- Media Access Control hardware address (e.g., 48 bit address on a network interface card).

Mobile Asynchronous Communications (MASC) protocol, which is the standard form of communicating between a Mobitex wireless data subscriber device and the computing platform. MASC allows applications developed on the computing device to provide high levels of control and management of the wireless modem. The MASC protocol is used when developing highly efficient, commercial wireless application software.

Mobitex - Ericsson's Eritel subsidiary's cellular land-radio-based packet-switched data communication system. Used by RAM mobile data. The raw data transmission bit rate was originally 8,000 bits/s (using 512-byte packets) for all installations, which provides a user data throughput of about 2.4 to 5 kbits/s, but this has been upgraded to 19,200 bits/s in some larger cities. Usage charges are per kilobyte. More open that the competing Ardis system, since all specifications are developed by the Mobitex Operators Association. Was designed by L.M. Ericsson and Swedish Telecom. Uses 896 to 901 MHz and 935 to 940 MHz. Cantel offers the service in Canada. Available in about 11 countries, but different frequencies are used, so roaming is complicated. L.M. Ericsson server is http://www.ericsson.nl/. (Taken from O'Reilly.) Return to Table 6.

Network - 1. A configuration of data processing devices and software connected for information interchange. 2. A group of two or more computer systems linked together.

Network Operating System (NOS) - Software that is used to link files, computers, and other devices over a LAN or WAN.

NIC - Network Interface Card. A hardware device used to connect computers to a wired or wireless network.

Obsolescent- A technology or protocol rating used in this document. Definition: "The Client Enterprise Architecture actively promotes that agencies employ a different technology. Agencies should not plan new deployments of this technology. Agencies should develop a plan to replace this technology. This technology may be waning in use or no longer supported."

Open Group, The - An international consortium of computer and software manufacturers and users dedicated to advancing multi-vendor technologies. The Open Group was formed from two previously independent groups - the Open Software Foundation (OSF) and X/Open Company Ltd. The Open Group maintains standards for DCE.

Open System - 1. A system whose characteristics comply with standards made available throughout the industry and therefore can be connected to other systems complying with the same standards.

OSI - Open System Interconnection.

OSI 7 Layer Model - An ISO standard for worldwide communications defining a framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

Packet - A collection of payload data and transport information that is transmitted as a bundle across a network connection.

Packet Switching - The process of routing and transferring data by means of addressed packets so that a channel is occupied only during transmission of a packet. On completion of the transmission, the channel is made available for transfer of other packets.

Patch Panel- An assembly of pin locations and ports, mounted on a rack or wall bracket. A patch panel acts like a switchboard where cable from throughout a building can be connected together to form a local network or to the outside linking to the Internet or other wide area network.

PBX - Private Branch Exchange – a premise voice switch.

PCI - A standard for connecting peripherals to a personal computer, designed by Intel and released in 1993. PCI is supported by most major manufacturers.

PCS- Sprint's Personal Communications Services. It operates in the 1.9 MHz band. It is not a cellular service. (600mhz, 900mhz) Return to Table 6.

QoS-Quality of Service - The performance of a network service such as throughput, delay, and priority. Some protocols allow packets or streams to include QoS requirements (e.g., ATM).

RAID - Redundant Array of Independent Disks. A method of organizing small format disk devices to drastically increase I/O bandwidth and improve data availability.

RAM Mobile Data- a wireless service. A company jointly owned by RAM Broadcasting, Inc., Ericsson, and BellSouth Corp. that provides a cellular-radio -based packet data service called Mobitex. Competes with Ardis and CDPD. Ericsson encourages others to manufacture compatible equipment (people prefer an open standard). (Taken from O'Reilly.) Return to Table 6.

Remote Monitoring (RMON) - Standard providing packet collection, decoding, and analysis to a layer of the operating systems interconnection stack, using a combination of consoles, hardware and software probes that rely on SNMP MIB data collection. The combination of RMON and SNMP provides powerful network diagnostic tools that facilitate multi-vendor interoperability.

Router - 1. An attaching device that connects two LAN segments, which use similar or different architectures, at the reference model network layer. 2. (IRM) The combination of hardware and software that links LANs and WANs together.

Segment-1. vt. to isolate traffic on a LAN; 2. n., the LAN devices and media isolated.

Simple Mail Transport Protocol (SMTP) - The standard transport protocol for sending messages from one MTA to another MTA over the Internet. Using MIME encoding, it enables the transfer of text, video, multimedia, images, and audio attachments through e-mail messages.

Simple Network Management Protocol (SNMP) - A set of network communication specifications that cover all the basics of network management. It is a simple and expandable protocol designed to give the capability to remotely manage a computer network by polling, setting terminal values, and monitoring network events. It is comprised of three elements, an MIB, a manager, and the agents. The manager is located on the host computer on the network. Its role is to poll the agents and request information concerning the networks status. Agents run off each network node and collect network and terminal information as specified in the MIB.

SLANI-State and local government network integration subcommittee of COTS (1998-2000)

SMDS - Switched Megabit (or Multi-megabit) Data
Service

SPX- Sequenced Packet Exchange. An OSI layer 4 protocol or transport layer protocol built on top of IPX. SPX is used in Novell NetWare systems for communications in client/server application programs.

Star Topology - A network LAN infrastructure in which each node is connected to a central hub.

Strategic- A technology or protocol rating used in this document. Definition is " The Client Enterprise Architecture promotes use of this technology by agencies. New deployments of this technology are recommended."

Switch- 1. n., a circuit switching hub. 2. vt., A communications paradigm in which a dedicated communication path is established between the sender and receiver along which all packets travel. The telephone system is an example of a circuit switched network. Also called connection-oriented.

Synchronous - Two or more processes that depend upon the occurrences of specific events such as common timing signals.

Synchronous Optical Network (SONET) - 1. A new and growing body of standards that define all aspects of transporting and managing digital traffic over fiber-optic facilities in the public network. 2. A network communication technology offering fiber optic transmission system for high-speed digital traffic.

T1-An AT&T term for a digital carrier facility used to transmit a DS1 formatted digital signal at

1.544 megabits per second or a 24 analog line equivalent. T1 transmission uses a bipolar Return To Zero alternate mark inversion line coding schemes.

TCP-Transmission Control Protocol. An OSI layer 4 protocol

TDMA- Time Division Multiple Access

TIA-Telecommunications Industry Association. A standards body. An association that sets standards for communications cabling.

Token Ring – An IEEE 802.5 standard for media access. Conflicts in the transmission of messages are avoided by the granting of "tokens" which give permission to send.

Transitional- A technology or protocol rating used in this document. The Client Enterprise Architecture promotes other standard technologies. Agencies may be using this technology as a transitional strategy in movement to a strategic technology. This technology may be waning in use or no longer supported.

TSB- Standards for testing and certifying telecommunications cables. E.g., TBS67

Tunneling – enveloping one protocol in another. E.g., packaging an un-routable protocol inside a routable frame.

Wide Area Network (WAN) - 1. A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan area network, and that may use or provide public communication facilities. 2. A data communications network designed to serve an area of hundreds or thousands of miles; for example, public and private packet-switching networks, and national telephone networks. 3. (IRM) A computer network that links multiple workstations and other devices across a large geographical area. A WAN typically consists of multiple LANs that are linked together.

X.25 - The CCITT protocol standard for connecting to packet-switched networks. Typically used to connect wide area networks, packet switching breaks network data into smaller packets and sends the packets from point to point through interconnected switches.

Information provided in this Glossary was liberally borrowed from a number of Internet sources including the following highly recommended sources:
O'Reilly's (search box at the bottom of the page) http://www.oreilly.com/reference/dictionary/tsearch.cgi
What Is? http://whatis.techtarget.com/
Cisco's Glossary of LAN terms http://www.cisco.com/univercd/cc/td/doc/product/lan/trsrb/glossary.htm
MobilInfo.Com Glossary http://www.mobileinfo.com/Glossary/
Free Online Dictionary Of Computing http://foldoc.doc.ic.ac.uk/foldoc/index.html
North Carolina ITS Glossary http://www.its.state.nc.us/Information/Glossary/GlossMain.asp
U. of Colorado Computing Standards with Links http://itp-www.colorado.edu/~scig/std_glossary.html

Appendices

Appendix A. Network Domain Team Analysis of Technology Trends, Enterprise Business Strategies and Requirements for Technical Architecture

Network Domain Team Analysis of Technology and Business Trends

The future technical architecture of the Client, in the absence of architectural plans, will be shaped by technology trends. The Enterprise Architecture Work Group identified trends they believed to have potential for significant impact on the way the Client does business. The network domain team looked at these trends and alsoconsidered trends that were specific to the domain. These are discussed below.

The network domain team identified four critical technology trends that will shape networking in the future. These critical trends are as follows:

- Bandwidth needs will increase geometrically as data, voice and video converge to everything over IP (EoIP).
- Bandwidth needs will continue to exceed availability on average, thus driving the need for improved end-to-end quality-of-service controls in LAN and WAN communications, whether cabled or wireless.
- Wireless communications will escalate and will blur the lines between public and private communications.
- Remote infrastructure, remote network management services, and remote management of selected in-house services will change the way we design and build our networks.

The network domain team also reviewed the general technology trends that were identified in early 2000 by the Council on Technology Services (COTS) as having potential for a significantly affecting the Enterprise Architecture of the Client.These trends are viewed as having different levels of importance to the development of each technical infrastructure domain. The network domain team assigned domain development impact ratings to the COTS trends as follows:

- Higher Impact—these trends have significant potential for influencing near-term and long-range changes in network infrastructure
- Medium Impact—these trends influence some aspect of networking
- Lower Impact—these trends are related to networking but do not drive network architecture decisions.

Table 1: Domain Development Impact of COTS General Technology Trends

Higher Impact	Medium Impact	Lower Impact
TT01—Widespread access to the Internet by citizens	**TT04—**Network centric computing	**TT03—**Requirements for secure connections over the Internet
TT02—Internet and Intranets as dominant communications vehicles	**TT09—**Enterprise servers	**TT06—**Emergence of Web browser as client of choice

Higher Impact	Medium Impact	Lower Impact
TT05—Electronic commerce expectations of business partners	**TT13—**Enterprise Portals (e.g., bandwidth balancing issues among the several participants in portal information and services)	**TT07—**Technical Workforce shortage
TT08—Standardization on TCP/IP		**TT10—**Organizational dual discipline proficiency
TT11—Convergence of multimedia applications and networks		**TT15—**Increasing use of data warehouse technologies
TT12—Right-sourcing		**TT17—**Customized service delivery
TT14—Mobile connectivity		**TT19—**Standardization of desktop workstations
TT16—Rapid technology change		
TT18—Continued growth of OLTP		
TT20—Application hosting		
TT21—N-tier computing		
TT22—Systems management and support		
TT23—Technology price performance curve		
TT24—Availability of packaged solutions (Buy vs. build)		

The 13 higher impact COTS trends in Table 1 support and underscore the notion that bandwidth requirements will exert a driving influence on the Client's network architecture of the future. Mobile computing too is confirmed as an important influence. As we move to a more Web-enabled government, integrate voice, video and data services, and begin to access remote services to address our application needs, these and other uses of networks will fuel the growth in bandwidth requirements. From past experience, we also know that unanticipated user acceptance of services offered can consume available bandwidth well ahead of schedule. The phrase "build it and they will come" rings a familiar note in our present-day planning sessions. We need only look back and see that the expected life of category 5 cabling has fallen a bit short of our predictions due to functions such as printing. And we were caught envisioning a paperless world!

Network Domain Team Analysis of Enterprise Business Strategies

At the time that COTS members were evaluating technology trends, they also delineated the Client's Enterprise Business Strategies for 2000 and beyond. Because it is crucial that the network architecture support any requirements implied by these critical strategies, the domain team carefully appraised the impact each strategy might have on the overall decisions regarding changes in network architecture.

- Higher Impact—these strategies have significant potential for requiring near-term and/or long-range changes in network infrastructure
- Medium Impact—these strategies influence some aspect of networking

- Lower Impact—these strategies make relatively few demands on the network infrastructure.

Table 2: COTS Enterprise Business Strategies

Higher Impact	Medium Impact	Lower Impact
EBS01. Focus on Customer Service (especially continuity and reliability issues).	EBS02. Improve the Quality of Information and Decision-Making.	EBS04. Attract, Manage, and Retain a Highly Skilled Government Workforce.
EBS03. Respond to the Needs of a Growing, Diverse Population.	EBS07. Provide a Technically Educated Workforce. (e.g., paths for upgrading distance learning).	EBS05. Balance Freedom of Information with Privacy and Security.
EBS06. Identify and Encourage Improved Service Delivery Mechanisms.	EBS12. Promote Collaboration and Cooperative Systems Development.	
EBS08. Promote Continuous Improvement.		EBS09. Improve Procurement of Goods and Services
EBS10. Insure IT Interoperability.		EBS14. Reduce Gap between Availability and Adoption of Technology.
EBS11. Optimize Service Delivery through Improved Stewardship of Limited Resources (e.g., promotion of standards).		

Looking across these business strategies, the impact of changing customer expectations on the network architecture becomes clear. The Client's custome rs, whether citizens, business partners, internal agency staff or external agency personnel, will expectmore services, speedy service, high quality services and integrated services through their network connections. These expectations will drive network improvement decisions.

Network Domain Team Analysis of Requirements for Technical Architecture

The Enterprise Architecture Workgroup, by delineating information requirements related to the identified business strategies discussed above, developed a list of specific requirements for technical architecture. These requirements were assessed by the network domain team for potential for impact on the network architecture. The results are provided in Table 3 below.

Table 3: Business Strategy Based Requirements for Technical Architecture

High Impact	Medium Impact	Low Impact
RTA01— The Enterprise Architecture must facilitate provision of information as a primary service of government in the information age. (Especially availability, universality and continuity.)	**RTA03**	**RTA06**

High Impact	Medium Impact	Low Impact
RTA02—The Enterprise Architecture must enable deployment of appropriate service delivery directly to customers using cost effective technologies.	**RTA04**	**RTA07**
RTA19—The Enterprise Architecture must provide a flexible and scaleable infrastructure to support rapid fluctuations in demand.	**RTA05**	**RTA08**
RTA20—The Enterprise Architecture must enable capacity, performance and configuration management, using real-time and historical metrics.		**RTA09**
RTA23—The Enterprise Architecture must support flexible implementation based on industry standards consistent with mainstream trends.		**RTA10**
RTA25—The Enterprise Architecture must facilitate collaborative development of applications and related technology projects by organizations whether or not physically co-located.		
RTA28—The Enterprise Architecture must facilitate implementation of a high capacity and high availability technology infrastructure in all parts of the Client, in cooperation with business and industry that will attract businesses to the Client and promote widespread economic growth.		**RTA11**
RTA29—The Enterprise Architecture must enable strategic prototyping of new technologies and rapid deployment of technologies and service delivery mechanisms determined to be effective, stable, and appropriate. (Rapid deployment implies readily available bandwidth.)		***RTA12**
		RTA13
		RTA14
		RTA15
		***RTA16**
		***RTA17**
		***RTA18**
		***RTA21**
		RTA22
		RTA25
		RTA26
		RTA27

* Require additional interpretation by the EA Team.

The requirements for technical architecture identified above as having a potential for high impact on the future network architecture again emphasize the availability of reliable, high quality connections for all customers who will depend on the services and

information provided to them via network infrastructure. Also emphasized are the requirements for flexible and scalable architectures. Networks will need to be responsive to both rapid increases and rapid decreases in bandwidth demand. Network performance monitoring and capacity planning tools and metrics, that will be described in the systems management domain will play a very important role in assuring responsiveness.

Appendix B: A Brief Explanation of the OSI 7 Layer Reference Model

OSI Layers		The applications you know are up here above layer 7 (e.g., PC Word, PC IE, PC Netscape, or C/S Billing). Both your applications and your operating systems interact with the network by using application layer protocols.	**Protocols/ Hardware**
7.	Application	Application-to-application communications such as inventory and sales applications interacting; system or enterprise management applications protocols; the protocols that are used by an application such as a Web browser to communicate over the network. Synchronous error detection supplied by protocols such as FTP.	HTTP, FTP, SNMP, SMTP. X.4 mail;
6.	Presentation	This layer negotiates syntax between two communicating systems at the start of a session to insure that what is transmitted may be translated to whatever the application layer needs to have meaning. Translation protocols. (Takes what the layers below deliver and translates it to what the layer above needs. Example: encryption/decryption; ASCII, EBCDIC; terminal type translations.)	X.4 mail
5.	Session	Each session connection knows only one transport connection. The session layer handles the dropping and adding of sessions to maintain a class of service. The two way flow of information is synchronized here.	Zone Information Protocol (ZIP)*;* and Session Control Protocol (SCP).
4.	Transport	Maintains class of service such as batch or interactive, connection or connectionless. Keeps flow of communications going by controlling the size of packets sent. For each transport connection, there is one simultaneous but possibly multiple sequential session connections.	TCP; SPX
3.	Network	Routing and addressing.	IP; IPX; routers
2.	Data Link	Asynchronous error detection; divides data into frames; flow control for frames; sequencing of frames; MAC addresses.	X.25; Ethernet; HDLC; bridges
1.	Physical	The sequence of events needed for the media to support communication between 2 open systems (computers). Media, mechanics, signaling,	Connectors, cable, repeaters, NIC, RS-232D

Middleware

Network

Appendix C: Emerging Trends and Issues in Wireless Networking

How Wireless Technologies Work

Wireless technologies:

- Employ a variety of **standards depending on the application**—e.g., IEEE 802.11(and 11a and 11b), wireless, GSM in Europe, HomeRF, GPRS, iMode, CDPD, etc. Many standards are under development such as CDMA 2000.
- Often use **radio frequencies** in the Industrial, Scientific and Medical 2.4GHz band (ISM)—a band used for many wireless applications. Other bands are used depending on the application (e.g., digital and analog cell phones use the 800 MHz range; and PCS operates in the 1850-1990 MHz frequency range.)
- Use 5 types of **signaling for LAN protocols**: direct sequence shared spectrum (DSSS), frequency hopping (FHSS), infrared (IR), high rate direct sequence HR/DSSS, and orthogonal frequency division multiplexing (OFDM). DSSS and FHSS are the main physical layer protocols presently in use. HR/DSSS and OFDM are for higher data rates.
- Use other **communication protocols**—any two communicating devices essentially establish a temporary mini-network that requires all of the network and middleware communication protocol types needed for node to node communications on a LAN or beween LANs. What is needed depends on the type of communication.
- Create signals by employing **modulation** techniques—how the information is encoded on the carrier signal is very important for throughput. High speed is gained by hanging more information on one waveform. E.g., 2 Mbps LANS use mainly binary phase-shift keying (BPSK) and quadrature phase-shift keying (QPSK).
- Use **access points—**which are LAN hardware devices that provide an antenna for communicating with nearby wireless devices that need to connect with a LAN.
- Use **embedded chips** —which are signal processors in the communicating wireless devices.

Wireless Uses and Trends

Wireless applications are expected to take off over the next few years. Prices will drop as use increases. Bluetooth is off to a slower than anticipated start. Most wireless networking applications are proprietary and do not interoperate.

- LANs (typically DSSS).
    - Example: a laptop connecting to a wired LAN using a wireless access method; using a wireless LAN to avoid defacing an historic building.
    - Maximum throughput is generally 11 Mbps for access point to access point (e.g., for a two building LAN) and 2 Mbps for device to LAN access point (distance dependant). Higher speed LANs are possible but more costly. Multiple point to point units may be used to improve throughput.
    - Each transmission from a wireless device is broadcast over several channels. This duplication provides a vehicle for error correction.
    - Usually use the ISM band with no hopping

  - Transmit Ethernet type packets
- WANs—wide area networks.
  - Example: 2 LANs connected between 2 buildings within line of sight.
  - Infrared point to point. Radio point to point.
  - Radio frequency private WANs—e.g., police communication systems.
  - Device to Internet—e.g., cell phones with Internet access capabilities.
- PANs—personal area networks
  - Example: a PDA connected to an office computer, a cell phone that can make regular (PSTN) phone calls when in the office, a headset that works with the phone, and a laptop that connects to the LAN all together are a PAN.
  - Radio Frequency (e.g., Bluetooth)
- Bluetooth (FHSS)
  - A set of wireless standards and protocols produced by an industry group.
  - Calls the mininetworks piconets (up to 8 devices) and scatternets (multiple connected piconets)
  - Maximum throughput is less than 1 Mbps in a 10 meter range
  - Broadcasts without checking for other users and can cause substantial interference
  - Uses ISM band divided into 79 channels hopping 1600 time per second
  - Connects a wide variety of devices with 13 narrow protocols tailored to what is communicating and what is being transmitted.
  - Because of rapid frequency hopping—dominates when in competition for the same airwaves.
- Wireless Internet
  - E.g., cell phone or Bluetooth connections to the Internet.
- Wireless Devices
  - Non-computing (e.g., 2 way radios, garage door openers, baby monitors, GPS, cordless phone, TV remote)
  - Computing (wireless keyboard and mouse, PC, laptop)
- Wireless Everything
  - E.g., Bluetooth chips in any two things that need to communicate such as a security alarm notifying the security company over the Internet or by phone.

Wireless Problems

- Transmission error rate is high requiring compensating mechanisms. Some contributing factors are heavy spectrum use, signal attenuation (signal weakening with distance), environmental noise, and multi-path
- Distance limits
- Throughput limits
- Bandwidth limits
- Lack of interoperability among wireless devices
- Security threats with bandwidth-eating security solutions
- Interference problems

- Battery conservation dimension to applications
- Most IrDA (infrared data) ports on computers do not work due to interoperability problems between the port and the software that wishes to use them.

Wireless Annotated References

Emerging Technology: Can Bluetooth Sink Its Teeth into Networking?
by Andy Dornan, Network Magazine, 11/05/00
http://www.networkmagazine.com/article/NMG20001103S0002
This article provides an historical perspective, substantial technical information and links for the Bluetooth approach to connecting everything to everything. Good diagrams (figures).

In-building Wireless LANs
ftp://ftp.netlab.ohio-state.edu/pub/jain/courses/cis788-99/wireless_lans/index.html
This paper provides a fairly in-depth look at wireless LANs including the 802.11, 11a, and 11b protocols, HIPPERLAN standards, and wireless LAN architecture. The author presents the next generation of wireless LAN standards. The Physical Layer and Media Access Layer are presented.

Wireless and Mobile Networking Terms by "What is"
http://whatis.techtarget.com/definition/0,289893,sid9_gci213380,00.html
Every imaginable wireless term discussed in considerable depth.

Technology tussle underlies wireless Web
By John Borland Staff Writer, CNET News.com, April 19, 2000, 11:30 a.m. PT
http://news.cnet.com/news/0-1004-200-1718810.html?tag=st.ne.1002
A discussion of protocol wars between Japan's iMote, and XML based technology for phone Internet connections and WAP, wireless access protocol.