U. S. Railroad Retirement Board

Network Domain Architecture

Network Domain Architecture
Table of Contents

Network Domain Architecture

Network domain describes the technologies, standards, and guidelines used to allow the reliable transmission of data* across various platforms for the use of employees, business partners, and customers.

*See glossary definition of data.

Domain Technology Categories

- Equipment
  - Switches, routers, hubs, muxs, firewall, modems, CSUs/DSUs, PBX
- Contractual communications services
  - Frame relay/ATM
  - VPN
  - Internet service provider
  - AT&T Global Network
  - IVR
  - Wireless communication
- LAN/WAN management
  - **Network services**
    - -Nortel (IVPN) user authentication
    - -MS Domain Name Service (DNS)
    - -MS Dynamic Host Communications Protocol (DHCP)
    - -MS Windows Name Service (WINS)
    - -MS Internet Information Server (IIS)
  - **Protocols and guidelines**
    - -TCP/IP
    - -IPX
    - -UDP
    - -FTP
    - -Telnet
    - -SDLC
    - -SMTP
    - -SNMP
    - -HTTP
    - -HTTPS
    - -Ethernet
    - -Token Ring
    - -Frame relay protocol
- Network connections
  - -Fiber (including Escon channel & Ficon)
  - -Copper (including UTP, STP, bus & tag)
  - -Wireless (in house)

Network Domain Principles Summary

1. Use, support, and integrate Enterprise Wide Technical Architecture (EWTA) as it relates to the Network Domain.
2. Sustain reliable connectivity.
3. Keep abreast of new technologies and develop and maintain the capacity to integrate them into the RRB's network infrastructure.
4. Consider impact on business partners.
5. Business requirements should govern the network technical architecture.
6. Network technical architecture must be extensible and scalable and be sustained to reduce integration complexity.

Domain Relevant Trends

- Wireless technology will be a future consideration
- Decreasing costs for components
- Increasing overall costs for the RRB
- Increasing capacity
- Increasing demands
- Increased network availability is expected
- Moore's law will continue to be valid
- Value provided by the network increases exponentially with increased utilization
- Value provided by the network reeds dependency
- Remote users will become more numerous therefore increasing pressure on connectivity and reliability

Background of Network Technologies at the RRB

The RRB's earliest data communications "network" began in the early 1970s and consisted of a mainframe computer connected with a limited number of 3270 terminals located in a central location. In 1980 coaxial cable was extended to each floor of the headquarters building. This enabled employees to have limited on-line access to payment history and certain other information, a significant improvement over the microfiche previously depended on.

In 1984 network data access was extended to every field office providing at least one 3270 terminal. During 1986 the first PCs with 3270 emulation cards became available on a limited basis allowing greater functionality to the mainframe network. By 1989 each headquarters employee had a 3270-type terminal, providing expanded access to mainframe-stored data.

In 1993 the first limited, segmented LANs were installed at headquarters allowing file sharing, printer sharing, and improved communications within each LAN. In 1994 PC/host gateways were introduced providing low-speed access to the mainframe without requiring 3270 emulation hardware. By 1996 there were 26 segmented networks in headquarters. By 1997 segmented LANs were installed in 24 field offices.

During early 1996 the Interactive Voice Response (IVR) system was implemented under contract with AT&T. This allowed beneficiaries to obtain certain information 24 hours a day, seven days per week via toll-free telephone.

During 1997 the VLAN using 100BT core infrastructure was operational, interconnecting all headquarters-based segmented LANs.

In 1999 VLAN/LAN/WAN over frame relay installation was completed connecting all 54 field sites to headquarters. IP replaced IPX-based PC/host gateways, greatly improving network speed. Additional improvements were made in 2000 to replace the IP/PC/host gateways with direct connection to the mainframe's OSA2 internal router device.

During 2001, the gigabit fiber core infrastructure was installed providing expanded bandwidth, allowing for future growth. We are currently (6-2001) planning for installation of gigabit fiber connections between servers and the core infrastructure, improving connection speed.

The RRB now (6-2001) utilizes approximately 97 servers including the mainframe (enterprise server) connecting 55 locations to Cisco 6509 and 3524 series routers. Two LAN operating systems are currently in use: Windows NT 4.0 and Novell NetWare 4.2 (being phased out). End user workstations are capable of 100baseT. This structure supports approximately 1,100 users - 300 at 54 remote sites and 800 at the Chicago Headquarters. There are a growing number of mobile users. Support for all users is provided from the Chicago HQ. The agency anticipates supporting 150 mobile users this calendar year using a virtual private network (VPN). All agency users, mobile or fixed, have Intranet access.

Detailed Domain Principles

Domain Principle 1

Use, support, and integrate Enterprise Wide Technical Architecture (EWTA) as it relates to the Network Domain.

Rationale:

This principle defines the parameters under which other principles can be structured and applied.
EWTA development is mandated by law.
Compliance provides consistency within the network area.
Compliance supports the integration of the network domain with other RRB domain areas.

Implications:

Wiser spending decisions should result.
Greater alignments will be created between the network domain and business needs.
Allows the RRB to use a global approach to IT investment decisions.
Instills accountability in the decision-making process.
A longer decision-making process may result.
Final results of the decision-making process should be of higher quality with a smoother implementation.
Benefits will result from a greater coordination of various IT projects.
A learning curve may result as new processes are developed and applied.
Change management will become institutionalized.
A cultural adjustment will be required.

Domain Principle 2

Sustain reliable connectivity.

The network infrastructure should provide reliable connectivity between employees, customers, partners, and the enterprise information resources.

Rationale:

Users are increasingly dependent on the network for information access and to perform daily business functions. Lost employee productivity is costly to the agency. The highest possible level of service must be maintained for the RRB's external and internal customers.

Implications:

Anticipate increased overall costs.
Design to avoid single points of failure.
Provide proper staffing.
Ensure adequate training.
Acquire network management/monitoring tools.
Adhere to an equipment refreshment schedule.
Acquire adequate contractual maintenance support.
Equipment and service acquisition should consider reliability factors and weight them against associated costs.
Provide criteria for acceptable reliability for various network components and services.

Domain Principle 3

Keep abreast of new technologies and develop and maintain the capacity to integrate them into the RRB's network infrastructure.

Rationale:

This helps develop better solutions to current performance problems and to improve performance to meet increasing demands of the end users.

Legislative changes must be accommodated as well as addressing changing customer needs.

Implications:

Anticipate and budget for increased overall costs.

Provide proper staffing.

Ensure adequate training.

Adhere to an equipment refreshment schedule.

Provide adequate contractual support.

Equipment and service acquisition should consider reliability factors and weight them against associated costs.

Comply with the RRB approval process and the RRB's overall IT strategy and budget constraints.

Assess the availability of new technologies.

Maximize and exploit Internet and Intranet technologies and approaches.

Identify, evaluate, and adapt new technologies through a formalized change management process.

Domain Principle 4

Consider impact on business partners.

Business partners are defined as but are not limited to Federal, state, and local government agencies, outside vendors/suppliers, RR employees and claimants (including on-line services), RR employers, insurance companies, banks, Medicare contractor(s), Internet service providers, mobile users.

Rationale:

Certain partnerships are mandated by law.

Some partnerships are mutually beneficial.

Some partnerships sustain and improve business.

Some changes satisfy customer expectations.

Implications:

Support multiple data types.

Comply with data exchange protocols and standards.

Coordination with business partners and internal users will be necessary.

Protect against security vulnerabilities.

Consider utilizing Internet or other interfaces to provide connectivity advancements.

Include business partners and customers' requirements in the planning and implementation process.

Users must consider the impact of their decisions on the network. In planning changes with business partners, users should include network experts.

Domain Principle 5

Business requirements should govern the network technical architecture.

Rationale:

RRB business should not be constrained by the network.

The network should be appropriately sized to support anticipated RRB business needs.

Implications:

Support multiple data types.

Networks will be implemented in adherence with the agency's security, confidentiality, and privacy policies.

Anticipate possible change in total cost.

Develop a process where the network domain is attuned to business requirements.

Users must consider the impact of their decisions on the network.

Provide proper staffing.

Ensure adequate training.

End users make business requirements.

Use a forecasting process for trend analysis of end users' needs and network capabilities.

Domain Principle 6

Network technical architecture must be extensible and scalable while sustaining the design to reduce integration complexity.

Definitions:

- *Extensible: Having the ability to easily integrate new technology and functionality. As it applies to the network domain this means adding new functionalities.*
- *Scalable: Having the ability to quickly meet the demands for increased or decreased performance, processing power, network connectivity, or data storage. As it applies to the network domain this means changing capacity without new functionalities.*

Rationale:

The RRB needs the ability to quickly meet changing demands for system performance and functionality. Leverage the capital expenditures in network design to ensure future reduced integration complexity.

Implications:

Higher original costs should be anticipated.

Provide proper staffing.

Ensure adequate training.

Consider flexibility of equipment during procurement.

Establish Board standards based on industry standards for equipment to be acquired.

Take a long-term approach to system design and augmentation rather than a quick and easy approach.

Anticipate or forecast expected demands.

Preferred Domain Design or Configuration Patterns

Pattern 1

Continue to accommodate the increase in remote/mobile access needs (work-at-home and field remote access).

Purpose

Comply with Federal government and RRB directives for development of work-at-home initiatives. Satisfy desires of employees. Provide improved itinerant service capability for field personnel. Provides improved two-way communications between headquarters and business partners.

Applicability

Employees working at home.

Contact representatives performing itinerant service and employees in travel status.

Business partners and customers.

Access to the network from mobile devices within headquarters.

Assumptions

An increase in security will be required.
Increased connectivity flexibility through wireless technology will be needed.
Increased processing speed of network components (routers) will be needed.
Funding will be available.
Technology will be available.
Proper skill sets (includes training) will be available.

Cost effectiveness will result.

Improved two-way communications will result.

Structure Overview

See the Attachment 1 for “before” (the value-added network) and Attachment 2 for “after” (the VPN chart).

Detailed Pattern Description

Action items:
Provide training.
Develop migration plan from the legacy network.
Develop procedures & guidelines such as:

- Agency policy to acquire mobile/remote LAN access.
- Users instructions for installation and use of VPN access software.

Develop an action plan for increased helpdesk workload.
Continue acquisition of contractual communications services and other needs.
Establish and negotiate a service level agreement.

Benefits

Cost effectiveness will result.
Improved employee morale.
Reduced energy consumption.
Improved customer service.

Consequences

Increased vulnerability to security breaches.
Increased security costs.
Increased support costs.

Variations

None.

Related Patterns

Patterns 2 and 3.

Known Uses

Work-at-home and mobile users.

Pattern 2

Provide increased bandwidth to meet demands.

Purpose

Handle anticipated increases in traffic volume as a result of new technologies and increased use by SSA, RRs, the Internet service provider, field offices, etc..

Extend the network and network resources through the use of increased outsourcing of data and application resources.

Applicability

Applies to all internal and external users.

Assumptions

Funding will be available.

An efficient implementation plan would include:
--Procedures and guidelines.
--Coordination with business partners and internal users will be necessary.
--Include business partners and customers' requirements in the planning and implementation process.
Demand for increasing bandwidth will continue as a result of new technologies in support of imaging and distance learning,
Increase in security will be required.
Increased processing speed of network components (routers) will be required.
The number of high-end applications running on the WAN will increase.
Web-based programming will not be implemented in the short term.

Structure Overview

None

Detailed Pattern Description

Action items:
Provide training.
Develop migration plans from the legacy network.
Develop an action plan for implementation.
Continue acquisition of contractual communications services and other needs.
Establish and negotiate a service level agreement.
Consider implementation of the fastest connectivity in support of business needs. For example:
--High speed network access between field and HQ.
--Copper to fiber server connection evolution.
--Increased processing speed of network components (routers).

Benefits

Improved response time.
Greater leverage of existing programs. (Same programming can serve headquarters, field, customers.)
Increase process efficiency by providing file transfer protocol (FTP) facilities to external business partners.
A single version of a program can be accessed from across the enterprise.
Data can be accessed by business partners as close as possible to the source.
Internal work processes will be improved and streamlined.

Consequences

Communications line costs will increase.

Variations

None.

Related Patterns

Patterns 1 and 3.

Known Uses

Increased bandwidth to remote sites using contractual adjustment to aid in program development and service levels. Internet access was improved by increased line speed. The core backbone was upgraded from 100baseT copper to gigabit fiber.

Pattern 3

Take advantage of and acquire increased and improved connectivity and new technologies in order to increasingly merge the LAN servers and the mainframe platforms.

Purpose

Increase efficiency through resource sharing. Ensure connection between platforms is increasingly transparent to the end user. Data can be accessed as closely as possible to the source via high-speed connections.

Applicability

Applies to all internal and external users.

Assumption

Mainframe and LAN technologies will continue to evolve to integrate together.

Supplemental cross-platform training will be necessary.

Structure Overview

(WAN to applications printing diagram.)

Detailed Pattern Description

Action items:
Acquisition of open-standards hardware and software.
Develop detailed migration plan.
Coordinate and develop user procedures.

Benefits

Increased access to the enterprise server (mainframe).
Increase in speed and ability of resources being purchased (gigabit fiber capability).
Increased processing speed of network components (routers).
Would insure compliance with computer match agreement regarding data storage.
Improve data security and integrity though data duplication reduction.

Consequences

Cost to increase in speed and ability of resources being purchased (gigabit fiber capability).
Cost to increase processing speed of network components (routers).
Awareness training will be necessary for efficient use of agency integrated IT resources.

Related Patterns

Patterns 1 and 2.

Known Uses

Obsolescence of PC host gateways.
Mainframe applications printing across the WAN.
LAN server backup to the enterprise server.
Implementation of middleware services to provide access to mainframe data by the LAN or PC-based applications.
Implementation of HTTP protocol on the mainframe and on LAN servers.

Domain Participants

Domain Team Leader: Gerry Spencer (Alternate: James Fijolek)

Line of Business Representatives: Dan Fadden, Ronald Russo

Domain Participants: Thomas Kolavo, Curtis Mitchell, Keith Stennis

APG Representative: Judy Lombardo

Appendix 1: Domain Glossary

Term	Definition
ATM	Asynchronous Transfer Mode. The SONET standard for a packet switching technique which uses packets (cells) of fixed length.
Bus and tag	The original IBM channel developed in the 1960s incorporating copper multiwire technology. Capable of operating at 4.5 Mbps with a distance limitation of 125 meters.
Change Management	A set of techniques that aid in evolution, composition and policy management of the design and implementation of an object or system.
CSUs	Channel Service Unit. A type of interface used to connect a terminal or computer to a digital medium.
Data	Numbers, characters, images or other method of recording, in a form which can be assessed by a human or (especially) into a computer, stored and processed there, or transmitted on some digital channel.
Datagram	A transmission method in which sections of a message are transmitted in scattered order and the correct order is reestablished by the receiving workstation.
DHCP	Dynamic Host Configuration Protocol. A protocol that provides a means to dynamically allocate IP addresses to computers on a local area network. The system administrator assigns a range of IP addresses to DHCP and each client computer on the LAN has its TCP/IP software configured to request an IP address from the DHCP server.
Distance Education	Is a formalized teaching system specifically designed to be carried out remotely. The students and the teacher are in different locations and lectures are transmitted through some type of technology such as closed-circuit or public television or an interactive Web site.
DNS	Domain Name System. The distributed name/address mechanism used in the Internet.
DSUs	Digital Service Unit. A device used in digital transmission for connecting a CSU (Channel Service Unit) to Data Terminal Equipment (a terminal or computer).
Enterprise server	The mainframe has evolved to include client server functionality and thus the term mainframe is synonymous with Enterprise server.
ESCON	Enterprise Systems CONnection. ESCON is a high-speed input/output (I/O) interface for mainframe computer connections to storage devices. ESCON is an IBM fiber optic standard capable of a maximum channel link speed of 17 MBps simplex.
Extensible	Said of a system (e.g. program, file format, programming language, protocol, etc.) designed to easily allow the addition of new features at a later date through the use of hooks, an API or plug-ins.
FICON	FIber CONnectivity. FICON is a high-speed input/output (I/O) interface for mainframe computer connections to storage devices. FICON is an IBM fiber optic

Term	Definition
	standard capable of a maximum channel link speed of 100 MBps full dulpex.
Frame relay	A recently developed switching interface which operates in packet mode. Generally regarded as the future replacement for X.25.
FTP	File Transfer Protocol. The Internet protocol (and program) used to transfer files between hosts.
HTTP	HyperText Transfer Protocol. The client-server TCP/IP protocol used on the World-Wide Web for the exchange of HTML documents.
HTTPS	HyperText Transfer Protocol, Secure. A variant of HTTP used for handling secure transactions.
IEEE	Institute of Electrical and Electronic Engineers. A professional organization, which, as a part of its services to the community, performs some pre-standardization work for OSI.
IIS	Internet Information Server. Is intended to meet the needs of a range of users: from workgroups and departments on a corporate intranet to ISPs hosting web sites. Features include innovative web publishing, customizable tools, wizards, customizable management tools, flexible administration options, and analysis tools. IIS makes it easy to share documents and information across a company intranet or the Internet.
IP	Internet Protocol. The network layer protocol for the Internet protocol suite.
IPX	Internetwork Packet Exchange. The Novell Netware protocol that provides datagram delivery of messages.
ISO Seven Layer Model	International Organization for Standardization. Best known for the 7-layer OSI Reference Model.
IVPN	Internet Virtual Private Network. For data, the logical configuration of a group of hardware components that includes direct connection THROUGH (as opposed to TO) the Internet. Usually refers to a network in which some of the parts are connected using the public Internet, but the data sent across the Internet is encrypted, so the entire network is "virtually" private. This sort of arrangement allows certain users reasonable access to a fully operational corporate network via the Internet.
IVR	Interactive Voice Response. Is a software application that accepts a combination of voice telephone input and touch-tone keypad selection and provides appropriate responses in the form of voice, fax, callback, e-mail and perhaps other media. IVR is usually part of a larger application that includes database access.
Moore's Law	Named after a co-founder of Intel, states that the number of transistors (or the amount of memory) that can be placed on a chip doubles every 18 months. It was a prediction more than a "law" in the sense that a scientist would use it; the usage is tongue-in-cheek in the vein of Murphy's Law. Semiconductor manufacturers actually take this prediction quite seriously and use it for forecasting the type of technology that will be available. Most industry analysts, and Moore himself, expect his prediction to hold true for at least another two decades.
OSI	Open Systems Interconnection. An international standardization program to facilitate communications among computers from different manufacturers. OSI is a seven-layer model.
PBX	Private Branch Exchange. A telephone exchange used within an organization and located on the premises.
Protocol	A formal description of messages to be exchanged and rules to be followed for two or more systems to exchange information.
RG-62	A designation of coaxial cable used for 68 ohm, long run RF data broadcasting (radio) or for computer network transmission and reception in ARCNet installations.
RS-232	RS-232 defines the meaning of the different serial signals and their respective pin assignments on a standard 25-pin (DB-25) serial connector. Since RS-232 defines signals that are not used for most standard communication, sometimes DB-25 connectors are missing unneeded pins. In this case, serial cables simply leave the

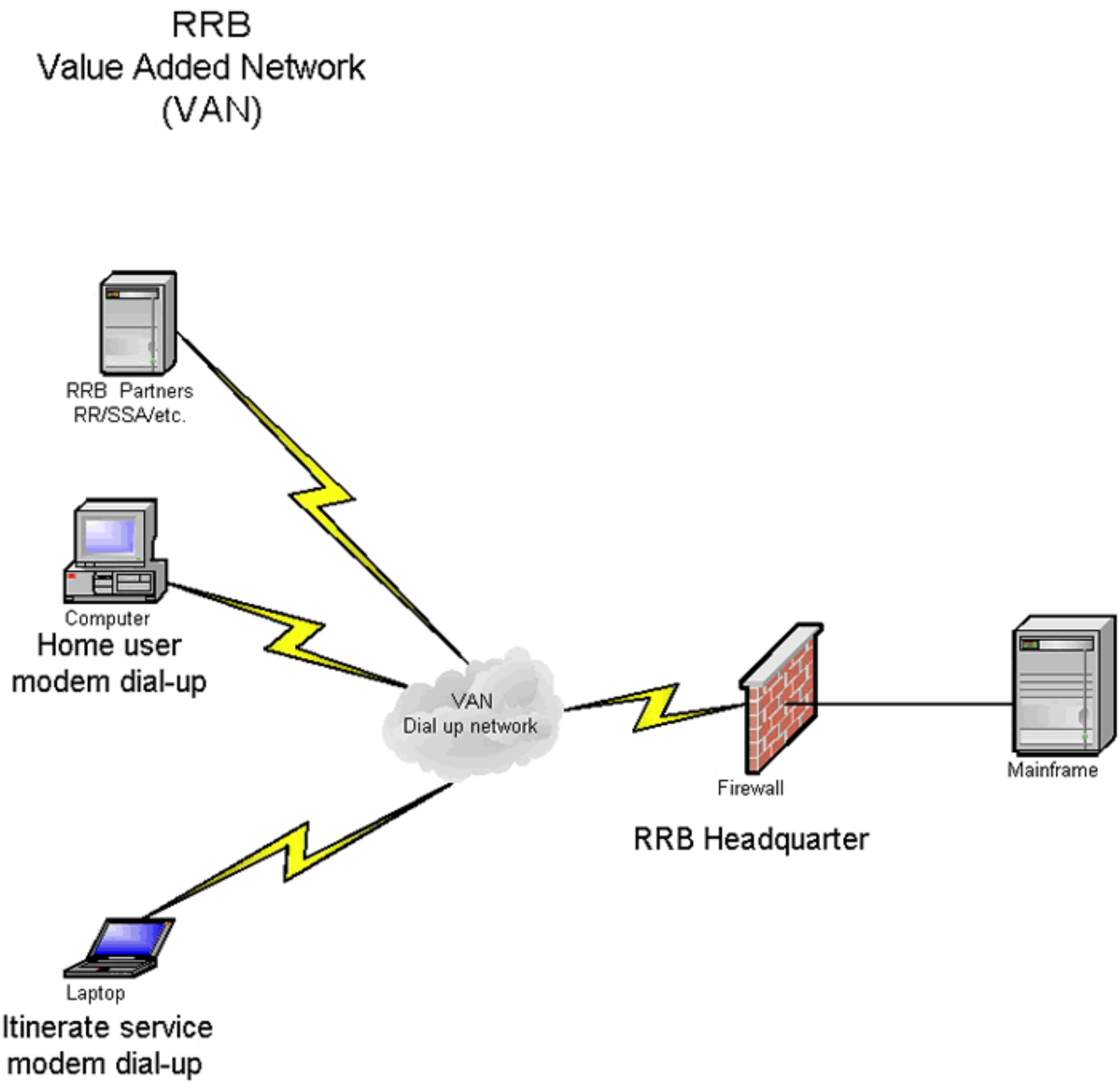
Term	Definition
	unused pins disconnected.
Scalable	The ability to quickly meet the demands for increased or decreased performance, processing power, network connectivity or data storage.
SDLC	Synchronous Data Link Control. A bit-oriented synchronous communications protocol developed by IBM where the message may contain any collection or sequence of bits without being mistaken for a control character.
SMTP	Simple Mail Transfer Protocol. The Internet electronic mail protocol.
SNMP	Simple Network Management Protocol. The network management protocol of choice for TCP/IP-based internets.
STP	Shielded Twisted Pair. A kind of cable used for most Ethernet cabling, especially fast Ethernet connections such as 100 Mbps.
TCP	Transmission Control Protocol. The major transport protocol in the internet suite of protocols providing reliable, connection-oriented, full-duplex stream. Uses IP for delivery.
TCP/IP	Transmission Control Protocol/Internet Protocol. See TCP and IP definitions.
Telnet	The virtual terminal protocol in the Internet suite of protocols. Allows users of one host to log into a remote host and interact as normal terminal users of that host.
Token ring	A type of local area network that uses the token passing access method and arranges the computers in a ring sequence.
UDP	User Datagram Protocol. A transport protocol in the Internet suite of protocols. UDP, like TCP, uses IP for delivery; however, unlike TCP, UDP provides for exchange of datagrams without acknowledgements or guaranteed delivery.
User authentication	The process of identifying a user through a unique identifier and allowing network access based on verification of identity.
UTP CAT 3	Unshielded Twisted Pair – Category 3. The cable used for some computer-to-computer communications. Maximum data rate 16 Mbps. Category 3 was the standard cable used for networking until 1993 brought the category 5 standard out. It was a high grade type 3, used for 4MBPS TR and 10MBPS Ethernet. It has 4 pairs with 3 twists per foot. Most telephone networks (POTS) use this cable today.
UTP CAT 5	Unshielded Twisted Pair – Category 5. The cable used for some computer-to-computer communications. Maximum data rate 100 Mbps. The category 5 standard states the twisted pairs must have at least 8 twists per foot. The general standard also (very) loosely implies that this cable should handle frequencies of 100MHZ or better.
UTP CAT 5E	Unshielded Twisted Pair – Category 5E. The cable used for some computer-to-computer communications. Enhanced category 5 cable, same specifications as UTP CAT 5 except that this cable handles frequencies of 200MHZ and most enhanced category 5 cable has 12 twists per foot.
WINS	Windows Internet Naming Service. Software which resolves NetBIOS names to IP addresses .

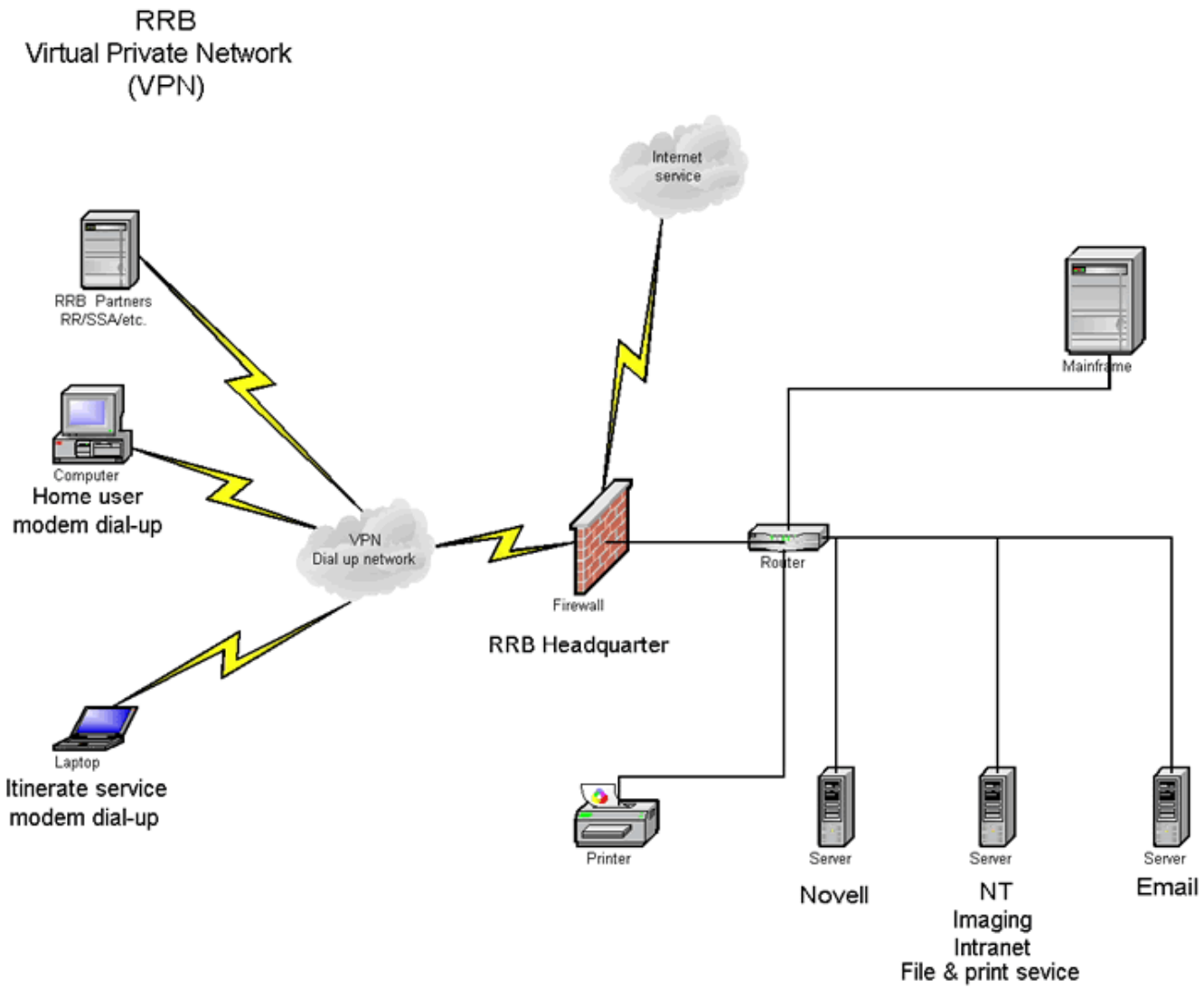
Appendix 2: Conceptual to Domain Principle Matrix

	Relationship Between RRB's Domain Principles And Conceptual Architecture Principles																								
Domain Principle	***Conceptual Architecture Principles***																								
	CA1	CA2	CA3	CA4	CA5	CA6	CA7	CA8	CA9	CA10	CA11	CA12	CA13	CA14	CA15	CA16	CA17	CA18	CA19	CA20	CA21	CA22	CA23	CA24	CA25
D-1	X	X	X																						
D-2															X							X			X
D-3													X		X					X			X		X
D-4										X												X	X		X
D-5				X						X															
D-6					X	X																			

Conceptual Architecture Guiding Principles:

1. Use guidelines consistent with the Federal Enterprise Architecture. 2. Support a single Enterprise Wide Technical Architecture (EWTA). 3. IT projects are to be consistent with the Enterprise Architecture. 4. IT projects are to be consistent with the Enterprise Architecture. 5. Reduce integration complexity. 6. Technical architecture must be extensible and scalable. 7. Manage information and data as enterprise-wide assets. 8. Validate information as close to its source as possible. 9. Enhance the ability to capitalize on and exploit business information. 10. Support multiple data types. 11. Make an informed buy versus lease versus build decision before proceeding with any new development project. 12. Require shorter development cycle times. 13. Keep current with emerging technologies and their applicability to enterprise architecture. 14. Maximize infrastructure asset reuse. 15. Sustain reliable connectivity. 16. IT systems will be implemented in adherence with the agency's security, confidentiality and privacy policies. 17. The agency will use a consistent set of security interfaces and procedures. 18. Reduce total cost of operation (TCO). 19. Extend E-Mail to Become a Corporate Information Exchange Vehicle. 20. Adopt Open Systems Standards. 21. Reduce duplicate information systems. 22. Reduce duplicate information systems. 23. Maximize and exploit Internet and Intranet technologies and approaches. 24. Integrate Enterprise Architecture into the investment management process. 25. Customer perception is a measure of the quality of the automation processes.


RRB
Value Added Network
(VAN)
RRB Partners
RR/SSA/etc.
Computer
Home user
modem dial-up
VAN
Dial up network
Firewall
Mainframe
RRB Headquarter
Laptop
Itinerate service
modem dial-up


RRB
Virtual Private Network
(VPN)
Internet service
RRB Partners
RR/SSA/etc.
Computer
Home user
modem dial-up
VPN
Dial up network
Firewall
RRB Headquarter
Router
Mainframe
Laptop
Itinerate service
modem dial-up
Printer
Server
Novell
Server
NT
Imaging
Intranet
File & print sevice
Server
Email