JUNE 2004

Technology Backgrounder on Data Networking Basics

By Larry Hettick and Steven Taylor

Today's telecommunications expert cannot survive without also becoming today's data networking expert because the convergence of voice and data networks has arrived. Converged networks have already become standard operating procedure for service providers, and they are becoming the standard for large enterprises. Converged networks also offer a great opportunity for small and medium businesses (SMBs). Acting as an effective equalizing factor, the SMB can now have a "big business" persona while preserving its inherent agility and personal service.

This backgrounder is designed to help the SMB telecommunications expert learn a few data communications basics, allowing these businesses to compete on a level playing field along the road to understanding network convergence.

Produced By: Webtorials

Sponsored By: NORTEL NETWORKS™

Protocols

Much like diplomatic protocols determine the rules of conduct by which diplomats conduct affairs of state, data communications protocols determine the rules for data format and transmissions.

Data protocols also work together in layers. Historically, discussions of data communications protocol layers start with a discussion of the Open Systems Interconnect (OSI) Model. The good news about the OSI model is that it provides a framework for assigning logical functions to various network components using seven "layers." The bad news, however, is that while the OSI model is intriguing from an intellectual perspective, few network functions today fit neatly into one of the seven layers. For this reason, we will define the network layers here according to common usage today rather than adhering strictly to the OSI model.

Layer 1, also called the physical layer, provides for physical connection including both hardwired and wireless connection protocols. Examples of a physical layer protocol include standards for physical connectors like RS-232 or RJ-11. The electrical characteristics of how information is transmitted over a wire are also physical layer concerns.

Layer 2 protocols specify ways to assemble information (like digitized voice signals or email attachments) into discrete packets. It's called the "link layer" because the specifications are limited to a single point-to-point link as opposed to an end-to-end connection. Ethernet and frame relay are commonly considered Layer 2 protocols.

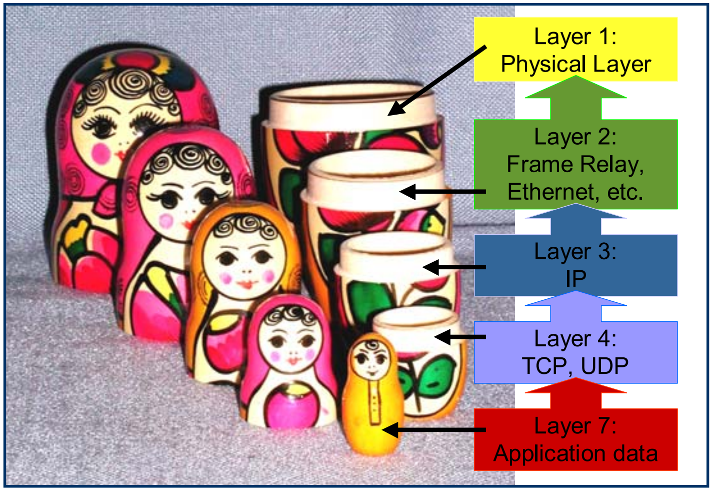
Layer 3 defines end-to-end addressing for packet protocols, much as a letter is addressed. When "Layer 3" is used today, it typically refers to Internet protocol (IP).

Layer 4 assures sure that the end-to-end communications session between devices is properly managed, and includes responsibility for packet error detection and correction. Transmission Control Protocol (TCP) is an example of a layer 4 protocol.

These first four layers are the most important for the purpose of this backgrounder. Layers 5 and 6 are not well defined and rarely discussed outside of an academic setting. Layer 7, called the applications layer, is enjoying increased attention. How to manage applications is an advanced topic - one that we'll no doubt discuss in another backgrounder.

As shown in Figure 1, all of these layers provide functions that are necessary for successful communications. Even though you may be using an "IP Network," for instance, this does not mean that none of the other protocols are in use. In reality, protocols tend to be used in a stack, much like a matryoshka, the nesting Russian doll.

Figure 1: Just like stacking dolls, the various protocol layers are added with each providing specific functions.



Ethernet

Devices within a local area may be connected on wires, over the air, or a mix of both. Ethernet, a layer 2 protocol, is the clear choice to the desktop. Ethernet specifications include rules for wireline data transmission rates at 10 Megabits per second (Mbps), 100 Mbps, and 1000 Mbps. The Ethernet specification is maintained by the Institute of Electrical and Electronics Engineers (IEEE). The IEEE family of Ethernet standards is called IEEE 802.3.

Although Ethernet was originally used only in the local area network (LAN), some service providers are offering Ethernet connectivity across an expanded territory within a metropolitan area. These services are referred to as Metro Ethernet.

Wireless LAN

Wireless LAN protocols, which are also layer 2 in the OSI model, are spelled out by the IEEE 802.11 family of standards. These protocols are often referred to as "WiFi." These standards include specifications for an over-the-air interface between a wireless client (like a wireless-enabled PC) and a base station or between two wireless clients. Wireless LANs can currently support connection speeds of 11 Mbps and 54 Mbps. Wireless LAN protocols are modeled after and compatible with the 802.3 Ethernet standards.

IP, TCP, and TCP/IP

As discussed above, Internet Protocol (IP) is a widely used layer three protocol. Originally developed to provide wide area network (WAN) connectivity, IP is now also used within a LAN to provide addresses for and control of intelligent devices like workstations, servers, and printers. IP is responsible for assigning addresses to individual data packets, with the IP addresses corresponding to the source and destination devices. Transmission control protocol (TCP) works together with IP. TCP is responsible for providing assured end-to-end communication by resending anything that gets lost and ensuring that packets are reassembled in the correct order. User datagram protocol (UDP) is a protocol similar to TCP that does not provide assured transmission. UDP is commonly used for the transmission of real-time information like voice and video.

Working together, TCP/IP protocols allow cooperating computers to share resources across a network. TCP/IP is also sometimes appropriately referred to as the "Internet protocol suite", since the Internet uses TCP/IP. Internet protocol standards are maintained by the Internet Engineering Task Force (IETF).

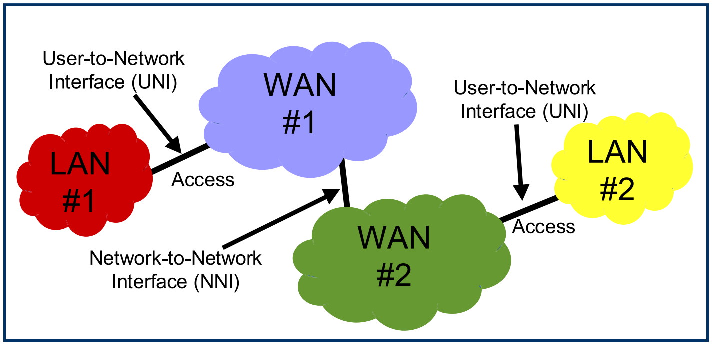
Frame Relay

Frame Relay (FR) is a WAN protocol that has enjoyed wide success as a more economical alternative to using private lines to connect LANs. Frame Relay is primarily a layer 2 protocol even though it has some layer 3 characteristics. Typically, the information that is carried by Frame Relay is TCP/IP traffic.

Building a Data Network

Data networks are built with three basic components: the Local Area Network (LAN), the Wide Area Network (WAN), and Access. These components are shown in Figure 2. Note that it is common in discussing data communications to use a cloud as an icon to represent a complex set of components that together form a logical network.

Figure 2: Data Network Component and Interfaces.


User-to-Network Interface (UNI)
WAN #1
User-to-Network Interface (UNI)
LAN #1
Access
LAN #2
Access
Network-to-Network Interface (NNI)
WAN #2

The Local Area Network (LAN)

The local area network, or LAN, has two options to connect at the physical layer. These options are a wired cabling infrastructure (usually twisted-pair cabling, similar to telephone cable) or a wireless infrastructure (which includes radio transceivers in access points and in computers). They can be used separately or together.

To send traffic between physical connection points in the LAN, networks can use shared media (like a LAN hub or wireless LAN) or can connect to dedicated resources like an Ethernet switch port. Most wired LANs have moved to a switched environment because of the enhanced ability to control an individual user's bandwidth consumption and quality of service.

Although wireless infrastructures are shared media infrastructures, wireless access points are typically connected to a wireline Ethernet switch port and then to physical cable. This hybrid environment offers a high degree of user mobility and, when properly engineered, also helps control the users' quality of service.

Setting up a LAN can be as simple as buying an Ethernet switch or wireless access point and connecting a site's workstations, servers, and printers with either Ethernet cable, wireless network interface cards, or both. Of course, a few simple configurations will be needed for installation but if the users can install software on PCs, then they can probably make the needed configurations. Plug and play, built-in self-discovery, and browser-based configuration tools make LAN installation much simpler today than a few years ago. Where required for more complex networks, the SMB can work with local resellers, service providers, or consultants to help with the planning and installation of the LAN. Once installed, service providers and resellers can provide ongoing management and support.

Access

To transport voice and data between LANs over a distance, the LAN connects to an access line, which in turn connects to a wide area network of some type. The access line can be a dial-up connection or a dedicated connection. Dial-up connections use modems to connect using the public switched telephone network (PSTN.) Dial connections have the advantage of being less expensive for the occasional connection; however, dial connections are limited to connection speeds ranging from 64-128 kilo bits per second (kbps.)

A dedicated connection is "always on." Dedicated options include private line connections using time division multiplexing (TDM), Digital Subscriber Loop (DSL), Cable Modems, and Metro Ethernet. The advantage of a dedicated connection is that it provides constant connectivity and can be less expensive at higher usage rates. Dedicated access speeds range from 64 Kbps up to multiple millions of bits (megabits or Mbps) per second.

Note that users can "mix and match" these access services to a common WAN core infrastructure.

The Wide Area Network (WAN)

To connect the LANs, users have the choice between service provider offerings that include dedicated services like private leased lines or packet services like Frame Relay and IP-VPNs. Wide Area Networks are typically a shared infrastructure offered by a service provider. For example, a dial access user will be connected by their dial access modem to another device across the WAN. A dedicated user can connect using a dedicated modem (like a DSL or cable modem) or another access device like a router.

A company can decide to use multiple access types as their needs for bandwidth may vary at different sites. For example, the user may elect to use a dial connection at a site with little traffic and a dedicated connection at a site with more traffic. The WAN will connect the two access links transparently.

WAN connections can also use the shared packet services or dedicated facilities within the carrier's network; the choice of shared vs. dedicated is up to the subscriber. Of course, dedicated facilities will cost more than shared facilities. Dedicated services can be either point-to-point or switched. Both of these options provide installation simplicity and yet may be priced higher than packet service options because the services cannot be shared among multiple users.

Packet services inherently share a WAN infrastructure. Frame Relay is a broadly deployed WAN service used by businesses of all sizes and is often considered to be a Layer 2 virtual private network (or VPN).

Users may also elect to use layer 3 IP-VPNs for WAN connectivity. These include using the public Internet or using a private VPN. The advantage of the public Internet is that it is less expensive and access is available from almost any location worldwide. The disadvantage is that added techniques (like IP-tunnels) are required to manage service quality and security.

The Internet is the most commonly used shared WAN. Internet connections require some kind of access, and traffic across the Internet uses multiple shared resources and perhaps even multiple shared networks to reach a destination. Since the Internet is a shared WAN resource, additional security measures must be taken, such as adding firewalls and/or secure socket layer and/or data encryption. These techniques and other measures like authentication should also be used if users are granted remote access to any VPN through dial-up connections.

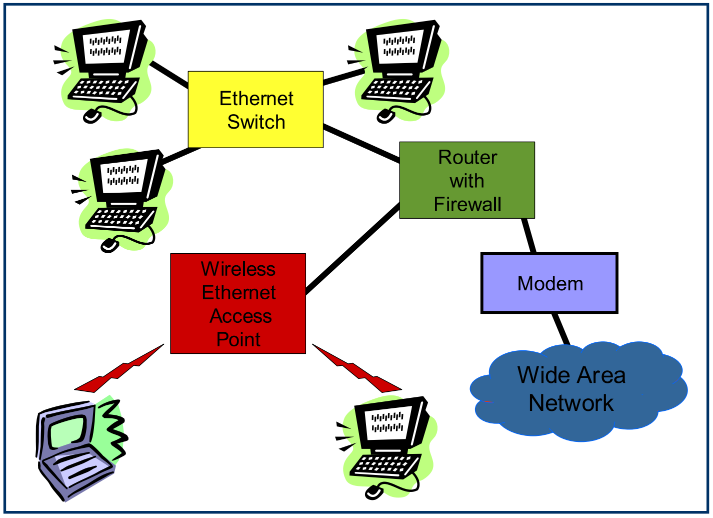
Private IP-VPN connections are a bit more expensive than using the Internet, but have some of the security measures and many traffic management techniques already built in to the service.

Data Networking Equipment

Unlike during the early days of networking, today it is common to have a single device perform multiple functions. So, while we'll list functionality by traditional device type, please keep in mind that these functions may actually be performed on a single device. Common premise-based data equipment, some of which is shown in Figure 3, includes:

- **Ethernet Hubs** provide shared cable media connections to Ethernet attached devices.
- **Ethernet Switches** provide a dedicated connection between Ethernet connectors like those found on a PC or Wireless Ethernet Access Point; replace shared media Ethernet hubs.
- **Wireless Ethernet Access Points** include an Ethernet 802.11 transceiver to send and receive wireless Ethernet traffic in the local area.
- **Network Interface Cards (NICs)** are used in a computer to send and receive traffic to the network. This device can also be implemented as a chip on the PC's motherboard.
- **Routers** filter and forward the IP packets to other IP-devices, including other routers
- **Modems** convert digital signals to analog signals so the information can be carried on an analog phone or cable network.
- **Firewalls** are hardware or software that prevents unauthorized access to a private network; they are a "must-have" when connected to the Internet.
- **VPN Appliances** are used to provide added security and performance for IP-based WANs, including the Internet. Can be used on premise and/or in the service provider's network.

Figure 3: Typical data networking equipment at a SMB site.



You will notice in these descriptions that the terms "switching" and "routing" are both used. In normal conversation, these terms are quite synonymous. In the data communications industry, "routing" usually refers to moving packets from device to device based on the IP protocol address while "switching" performs a similar function based on either a layer 2 protocol or the physical layer. However, this is not an exact rule.

While the list of data equipment and functionality may be a bit overwhelming to telecomm professionals, most of the hardware and software is relatively easy to install. Note that many of these devices can be installed and managed as part of a carrier's service offering. Choosing a managed service offering will also remove any pain associated with troubleshooting if users negotiate for end-to-end device and network management.

Final Considerations for Data Networks

Before making any build or buy decision for data networking, a business must also consider three important elements: management, security, and network resiliency.

Just as a business manager would assess how human or capital resources will be used before hiring or spending money, so too should an assessment be made about how a data network will be used. The assessment should focus on both short term and long term needs. If management is not experienced in assessing these needs and deploying the technology to address these needs, then calling in outside expertise will be money well spent. The business manager should also leverage any "free" expertise available from service providers and resellers who may want to bid on the data network. Questions for the assessment might include:

- How critical is data network uptime to my minute-by-minute business needs?
- What would happen if an outsider gets access to my information stored in the LAN?
- What skills do I have to buy or build a data network?
- When should I consider using my data network for voice traffic?
- How much employee time can I save with an efficient data infrastructure?
- How can I use my network to improve customer service?
- What's the bottom line return on investment?

Looking beyond the build or buy decision, the business must manage its data network just like any other resource. To shape a network management strategy, managers should ask themselves:

- How much of my data network is "self-managed" or "self-healing"?
- Who can I turn to if I have an immediate need or problem with the network?
- Am I willing to learn personally or dedicate employee time to manage this network?
- What's the bottom line return on investment for ongoing management?

Other decisions must be made about service level quality. Data networks can be designed to be as reliable as the phone network; however, the cost to assure phone-network levels of quality can be high. The secret to maintaining the right balance between costs and service levels lies in a sound service level agreement between the business and supplier. Managers are well advised to do some upfront research and to shop around for a service level agreement that meets business needs.

Data and data network security must also be considered when planning and operating a data network. Firewalls and encryption techniques can offer substantial security levels.

Additionally, management should consider how business policies, employment practices, and physical security can contribute to a safe and secure environment. Pre-deployment and ongoing security assessments are recommended for all enterprises.

Finally, the business management should also take resiliency and business continuity into account. Networks should have built in resiliency for day-to-day operations, and a disaster recovery plan should be in place before any potential failures or troubles occur.

Summary and Conclusions

Any business, no matter how large or small, must take advantage of effective information processing to succeed. To enjoy long-term success, the SMB must be able to compete with the same data-centric productivity tools used by larger enterprises. To enjoy lower operational costs, the SMB should also take advantage of advances in data networking and in the benefits offered by a converged network. Even though the SMB can rarely afford the data networking skills enjoyed by the large enterprise, some basic understanding about data networking, combined with help from strategic partners, can help the SMB compete on a level playing field.

Additional Resources

This backgrounder is one of a series targeted to help the small and medium business improve their skills in telecommunications and data communications. Additional backgrounders, papers, presentations, and detailed technical and business information are available from the backgrounder's sponsor and from www.webtorials.com.

Steven Taylor

Steven Taylor, consultant and broadband packet evangelist, is President of Distributed Networking Associates and Publisher of Webtorials. An independent consultant, planner, author, and teacher since 1984, Mr. Taylor is frequently quoted in the trade press and is one of the industry's most published authors and lecturers on high bandwidth networking techniques. He has served as a Contributing Editor for Data Communications magazine, publishes articles in both Business Communications Review and Network World, and co-authors two newsletters - Convergence and Wide Area Networking - distributed by Network World Fusion.

Larry Hettick

Larry Hettick has nearly 20 years of combined data communications and telecommunications experience. A capable and experienced speaker and writer, Larry possesses proven global expertise in product management and product marketing. Larry also writes for industry press, most notably as a co-author of Network World's bi-weekly Convergence Newsletter and as a periodic contributor to Business Communications Review. He is currently working as an independent consultant, specializing in the convergence market.

WEBTORIALS TECHNOLOGY BACKGROUNDER

Produced By
Webtorials, a venture of Distributed Networking Associates, Inc.
Greensboro, N.C.
www.webtorials.com

Design/Layout Artist
Debi Vozikis
dvozikis@rcn.com

For Editorial and Sponsorship Information
Contact Steven Taylor,
taylor@webtorials.com

Professional Opinions Disclaimer
All information presented and opinions expressed in this Webtorials State of the Market Report represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.

A word from the sponsor
Nortel Networks

By Diane Schmidt
Product Marketing Director for Data Networking, Nortel Networks

Nortel Networks data networking solutions solve today's infrastructure requirements while accelerating the evolution from simple connectivity to tomorrow's full convergence, delivering collaboration between employees, partners, customers and suppliers, where and when it is needed. With Nortel Networks broad portfolio of reliable and affordable, high performance data networking products, small and medium companies can accelerate their business success by increasing the resiliency and robustness of their communications infrastructures while also lowering costs and complexity.

Nortel Networks portfolio of data networking solutions for small and medium businesses include:

BayStack 325 and 425 Ethernet Switches are designed to provide high density cost-effective desktop switching, while providing scalability and ease-of-use.

Contivity VPN Switches provide low-cost secure connectivity to the Internet or managed IP networks. The compact, easy-to-manage platforms includes a high-performance IP-VPN, stateful firewall, URL/content filtering and optional integrated ADSL.

Passport 1600 Series Routing Switches are hardware-based Layer 3 Routing Switches that provide resiliency, performance and security in a compact design.

Wireless LAN 2200 Series provides a secure mobile networking environment featuring true mobility, strong encryption to protect user information, active security to protect the network, intuitive management, and full control of the radio resource for an enhanced multimedia experience.