

# Networking Fundamentals

This 2-day workshop introduces participants to the basics of data networking. The workshop begins with an overview of the issues involved in allowing computers to share information. It then describes the various types of networks that can be created and how they work. The section on network hardware focuses on the cables and interface devices used to establish connections between computers, identifying how each works and the role each plays within the network. In addition, the work of network connectors — repeaters, hubs, bridges, switches, and routers — and how they enlarge and interconnect workgroups is examined. An overview of network software is included, focusing on interface device drivers, network operating systems for peer-to-peer and Client/Server network operations, and network-specific applications. Finally, network design, implementation, and management issues are presented to illustrate how the components and concepts are used to build real networks.

## Who Should Attend

Candidates for this workshop should have some experience with using a computer but little or no knowledge of how computers communicate with each other. This group would include, but is not limited to, end users wanting to understand networks, desktop computer coordinators considering first time network installations, new network administrators, first-tier help desk analysts, programmers being introduced to networking, their managers, and others recently assigned to designing, installing, maintaining, or supporting digital networks.

## Prerequisites

This workshop assumes that the participant has used a stand-alone or networked computer, but has not been responsible for its setup or maintenance.

## Workshop Objectives:

- ▶ Become familiar with the basic issues for data networks, including industry terms and acronyms.
- ▶ Identify the types and functions of methods used to connect computers to allow them to share information.
- ▶ Learn how TCP/IP works, and how to configure it to various devices.
- ▶ Discover what hardware and software must be added to a computer to allow it to access other computers.
- ▶ Gain an understanding of how Ethernet works, and how all the various forms can be connected.
- ▶ Understand the roles and comparative uses of network repeaters, hubs, bridges, switches, routers, and gateways.
- ▶ Review WAN technologies.
- ▶ Recognize the interaction of device driver software, network operating systems, and network application programs.
- ▶ Survey the fundamentals of designing, implementing, administering, and managing networks.

# Implementing & Supporting Local Area Networks

Upon completion of this 2-day workshop you will understand the role of each of the hardware and software components that comprise a Local Area Network (LAN). A presentation of cable types, topologies, and wiring schemes will aid in evaluating your connectivity options. You will understand how CSMA/CD (802.3 and Ethernet) and Token Ring (802.5) hardware operates so that you will know what to expect when installing, administering, and troubleshooting these technologies. Network software features, configurations, and intersections will be discussed. After building a single conceptual LAN, we will discuss how LANs are connected using repeaters, bridges, routers, and gateways. Finally, you will also learn the basics of network security, management, and troubleshooting.

## Who Should Attend

Any individual with a (new) job description (such as LAN Administrator, Network Troubleshooter, Software Designer, or Application Developer) requiring a solid knowledge of modern network technologies, and will benefit from this systematic description of LAN components and concepts.

### Workshop Objectives:

- ▶ Identify the fundamental components of a Local Area Network.
- ▶ List the roles, features, advantages, and disadvantages of network connectors such as bridges, switches, and routers.
- ▶ Recognize the features and applications of coaxial, twisted pair, and fiber optic cables.
- ▶ Explain the basic probabilistic operation of CSMA/CD systems.
- ▶ Explain the basic deterministic operation of Token Ring systems.
- ▶ Discuss the broad areas of network security concerns and potential solutions in each area.
- ▶ Understand current network management alternatives, including the basics of SNMP and DMI.
- ▶ Present at least two ways of approaching a network troubleshooting problem.
- ▶ List and describe the use of instruments that could be used for testing a LAN.

# TCP/IP

This 2-day workshop provides participants both conceptual understanding and hands-on experience in deploying TCP/IP Network applications. This unique category of applications makes it practical and convenient for users to access a TCP/IP data network's resources. The workshop explores the vital TCP/IP services that run behind the scenes in order to make TCP/IP networks workable and practical: Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP), and Simple Network Management Protocol (SNMP).

This workshop is presented in classroom lecture/discussion style with hands-on labs to reinforce the lecture material. Students completing the class emerge with hands-on experience along with a workbook designed to serve as a practical reference tool.

## Who Should Attend

Personnel responsible for internetworking corporate resources: data center personnel, technical and communications managers, system and software engineers, LAN/WAN and network support technicians, systems and network analysts and designers, sales representatives and application engineers, information managers and LAN/WAN specialists, and application programmers who need a working understanding of LANs and TCP/IP.

## Prerequisites

General familiarity with data networks and the OSI Model.

### Workshop Objectives:

- ▶ Explain where these applications fit in the OSI Model, and how they relate to other applications and lower layers.
- ▶ Use the OSI Model as a troubleshooting tool, and as a way to quickly grasp new terms and technology.
- ▶ Build a running network using all three protocols we deploy in class (DHCP, DNS, and SNMP).
- ▶ Install DNS in Cisco routers, Windows workstations and servers.
- ▶ Activate SNMP network manager software and element agents in routers and Windows workstations.
- ▶ Explain how DHCP works and itemize its benefits and limitations.
- ▶ Compare DHCP to DNS and see where they complement and conflict with each other.
- ▶ Understand DNS address resolution, what forms it can take, where it is used and why it is so important.
- ▶ Use Windows-based TCP/IP testing and monitoring tools.
- ▶ Analyze DNS, DHCP and SNMP packets.
- ▶ Illustrate how the five functions of TCP/IP all work together to form the world's most popular network protocol suite.

# Data and Voice Networking over TCP/IP

This 3-day workshop builds a solid understanding of data and voice networking over TCP/IP from the ground up for personnel who have data and voice communications responsibilities. Students will work hands-on throughout the workshop and learn to use a variety of useful commands for checking response time, viewing current network statistics, and probing key services. Demonstrations with a network monitor/protocol-analyzer will enable the class to view and dissect network traffic.

Tracing is done via Ethereal which is Open Source Software, freely available to students via download. Hands-on commands used in the workshop include ipconfig, netstat, ping, tracertr/traceroute, arp, nslookup, whois, ftp, and views of security certificates.

## Who Should Attend

Network personnel responsible for the design, installation, maintenance, control center, and help desk support of IP data and voice networks. Typical participants include systems designers, engineers, network managers, service architects, product specialists, performance analysts, and support personnel responsible for voice and data networks, as well as vendor and service provider personnel. Systems managers, integrators, computer communications specialists and applications personnel also will find this workshop valuable.

## Workshop Objectives:

- ▶ Master the structure of TCP/IP and VoIP, and understand the implications for your data, voice, and media traffic flows.
- ▶ Obtain essential knowledge of how IP and VoIP traffic is encapsulated on LAN and WAN links, and how it can affect performance.
- ▶ Learn about manual and automated configuration options for network devices.
- ▶ Recognize the Quality of Service problems at each layer, and explore options for solving them.
- ▶ Analyze addressing plans, and find out about the IP address dilemma.
- ▶ Interact with a DHCP configuration server and DNS name server, and view the message exchange.
- ▶ See how IP network routes are selected.
- ▶ Use simple commands to get troubleshooting information fast, and learn how to use a free monitor tool to obtain error reports, capture traffic, and analyze network behavior.
- ▶ Master VoIP terminology and concepts for SIP or H.323 calls and softswitch components (e.g., Signaling Gateways, Media Gateways and Media Gateway Controllers).
- ▶ Walk through scenarios illustrating the steps in setting up VoIP calls and transmitting the payloads. Analyze SIP captures.

# Network Troubleshooting

This 3-day workshop is predicated on the fact that there are three major places where things can go wrong in a network: the workstation, the network itself and the server. The mornings of each day are devoted to understanding the network components in each platform, with specific focus on internal operating system troubleshooting tools available to isolate problems or point to the likely source.

Students spend afternoons debugging workstation and network problems, both single and multiple, per platform. On the morning of the third day, they learn how to isolate a problem to a server. The afternoon of the third day consists of mixed multiple bugs across all platforms which students are asked to find and fix. This last is the loose equivalent of a final examination. The expectation is that students will return to their jobs hoping that something can go wrong, so they can fix it!

This workshop is presented in classroom lecture/discussion style with hands-on labs to reinforce the lecture material. Students completing the class emerge with hands-on experience and a workbook designed to serve as a practical reference back on the job.

## Who Should Attend

Personnel responsible for internetworking corporate computing resources. This includes data center personnel, technical and communications supervisors and managers, system and software engineers, and LAN/WAN network support technicians.

## Prerequisites

Students are expected to have a working knowledge of TCP/IP data networking equating to about six months experience before taking this class. Familiarity with data network protocols, their operation and the OSI Model is assumed.

### Workshop Objectives:

- ▶ Use a standard problem-solving model when troubleshooting internetwork problems.
- ▶ Use and interpret the results of common network troubleshooting tools.
- ▶ Examine Cisco IOS diagnostic commands, analyze their meaning and take corrective action.
- ▶ Solve both LAN and WAN network problems.

# Network Security: Challenges and Solutions

This workshop is intended to provide network analysts with the basic tools needed to protect their computer networks. This 3-day workshop is normally presented as a combination of lecture, hands-on, and demonstrations. Clients hosting the class should discuss workshop customization and setup requirements with the workshop director.

Hands-on labs and demos include LAN setup, configuring IP, basic and extended IP commands such as PING, TRACERT and NETSTAT, using a LAN analyzer to examine IP packets, and using PingPro, NSLOOKUP, and WHOIS utilities on the Internet. Students will build Network Address Translation (NAT) and packet filtering firewalls in class.

## Who Should Attend

Personnel responsible for assuring the security of networked corporate resources: data center security personnel, technical and communications managers, system and security engineers, LAN/WAN and network support technicians, systems and network analysts and designers, sales representatives and application engineers, information managers and LAN/WAN specialists.

## Prerequisites

Students attending the class should be comfortable with the Windows environment and accessing the Internet. Some prior exposure to the TCP/IP protocol stack is also advisable.

## Workshop Objectives:

- < "Security is a process, not a product." — How to build a strong security process.
- < Understanding the non-technical issues: How much security is enough?
- < How to add security to voice and data networks.
- < How to recognize and repair network architectures that pose security threats.
- < Recognize and deal with Physical Layer security issues.
- < Recognize and deal with Data Link Layer security issues.
- < Be able to discuss weaknesses in the TCP/IP protocol suite: TCP, UDP and ICMP.
- < Know how to strengthen TCP/IP to acceptable standards.
- < Be able to explain the security implications of ICANN, ARIN, WHOIS and DNS utilities.
- < Explain the security built into VPNs, and how to pass VPNs through NAT and firewalls.
- < Explain how routing protocols relate to security, and how to make them more secure.
- < Know how to minimize the occurrence of time-wasting nuisances such as spam, adware, and pop-ups.
- < Be able to explain and implement best practices in web browser security.

# Best Practices in Network Security

Attaining a high level of network security is a matter of systematically implementing and maintaining the best security practices we can devise. This 2-day workshop trains participants in how to establish and maintain topnotch security in the face of ever more sophisticated threats.

Best Practices is presented as a combination of hands-on labs, demonstrations and lecture. Each unit has a full series of practical hands-on labs to reinforce the presented material. Labs include firewalls, use of authentication and encryption tools, implementing effective antivirus measures — and more — as noted in the following outline.

Attendees return to their jobs with a clear understanding of the security obstacles they face and armed with a powerful set of skills and tools to overcome them.

## Who Should Attend

The user community at all levels, user support staff such as Help Desk personnel, new employees as part of their orientation, data security personnel, LAN and network administrators, network support technicians, security analysts, security supervisors and managers, information managers and communications managers.

## Prerequisites

Students attending the workshop should be comfortable with any current Windows operating system.

### Workshop Objectives:

- ▶ Students learn why security has to be seen as a global process.
- ▶ Understand the role people play in the security package.
- ▶ Learn about firewall types, what they do, and where to place them.
- ▶ Explain intrusion detection principles and why they differ from firewalls.
- ▶ Discover what virtual private networks (VPNs) are, why they are so popular, and how to use them.
- ▶ Be able to compare and contrast authentication and encryption.
- ▶ Where encryption and authentication are best used to add security.
- ▶ How to detect and eradicate viruses and other malevolent code.
- ▶ Be able to use suppression software to minimize annoying spam, pop-up programs, and adware.
- ▶ Explain, practice and demonstrate sound web browser security practices.



# Wireless Networks: Theory, Practice and Security

This is a 2-day workshop covering all the major topics and issues involved in planning, deploying and managing wireless networks. Your attendance will expose you to the latest wireless theories and best-practices — including the 802.11 protocols, antennae specifications, architecture layouts, management, and security issues — in a multidimensional learning environment involving lectures, demonstrations with live wireless networks, examples and exercises.

The workshop will focus on applying the theory learned during the first part of the sessions with the practices of management, monitoring, and control of your organization's wireless environment. The examples and exercises will be oriented towards real-life situations in which the participants can incorporate their own experiences and get answers to questions concerning current problems and issues.

During the workshop sessions, the concepts of understanding the "what" and "how" of wireless network operation will be integrated with the "why" and "wherefore" of sound planning and management of such network infrastructures. Issues of wireless security, intrusion detection, and solutions will be prominent throughout the session discussions to ensure the participant's grasp of making their wireless environment safe and productive.

Participants are encouraged to bring laptop computers as there will be a limited number of wireless cards for use during the workshop so that everyone will be able to see and experience actual WLAN (wireless local area network) setup, management and intrusion detection situations.

## Who Should Attend

This workshop will be very beneficial to all those involved in an organization's wireless networking efforts: network administrators, technical support personnel, LAN administrators, system administrators, network security officers, MIS/IS/IT management personnel, and field support technicians. Technical and management personnel from organizations that have deployed wireless networks (or are planning on doing so) and would benefit from the current topics and issues discussed during the workshop sessions.

## Workshop Objectives:

- < Understand the wireless networking protocols currently being used and those in the development and standardization process.
- < Learn the different types of wireless network topologies from personal wireless architectures to metropolitan-sized unbounded networks.
- < Examine the theory behind the radio spectrum being used in today's wireless environments.
- < Learn how different types of antennae can impact the wireless network's performance and boundaries.
- < Dissect the different security protocols such as WEP, WPA, Kerberos, and TKIP.
- < Discover how wireless architectures can be chosen to match your organization's needs and requirements for improved coverage and security.
- < Using industry "best-practices", learn how to manage your wireless networks so that your organization can improve its TCO (total cost of ownership) of its wireless investment.
- < Learn the different wireless equipment components needed to deploy a complete network such as access points, wireless routers, firewalls, mobility cards, antennae, security devices, and authentication servers.
- < Understand the software components of a well-planned-out wireless network.
- < Discover how to develop a workable wireless network installation using an easy step-by-step network plan.
- < Uncover the necessary management skills and tools needed to assist in ensuring a wireless network that will provide an acceptable return-on-investment to an organization.
- < Learn the issues involved in wireless network security such as developing a security plan, understanding wireless vulnerabilities, and knowing wireless hacks and their perpetrators.
- < Discover how-to "hacker-proof" a wireless network to minimize down-time and lost productivity.
- < See actual wireless networks in operation under different configurations and layouts.



# High-Speed Networks

## High-Speed Options at a Glance

High-speed networks are the order of the day. The need for speed is the result of dramatically increasing usage of existing network applications, not to mention the addition of bandwidth-hungry applications containing voice, graphics and video. Data traffic has long since eclipsed voice traffic in terms of volume.

The solution is two-dimensional, having both WAN and LAN components, so this workshop covers both. We need more bits at a time, and must try to use all the bits we have. In the WAN sphere, T-carriers provide the bits; frame relay, ATM and TCP/IP help us use as many of them as possible. In LANs, we have Gigabit Ethernet and 10G Ethernet, both so rich in bits that economizing them is largely unnecessary. Digital Subscriber Line is also discussed from an access link perspective. Understanding each of these technologies and how they work together is the key to getting out of the bandwidth box.

Owing to the volume of information offered, this workshop runs for 3 days.

## Who Should Attend

This is an essential workshop for users, vendors and carriers who currently work with, or will work with, high-speed technologies. Those professionals who should attend include: LAN and WAN managers, technical staff, LAN and WAN administrators, network managers, network consultants, data communications professionals, telecommunications professionals, network architects, vendor sales, vendor marketing, and vendor applications staff, strategic and tactical is planners, carrier employees, and Internet service providers.

## Workshop Objectives:

- ▶ Gain a working knowledge of the T-carrier system.
- ▶ Learn how Frame Relay, the high-speed networking workhorse, works.
- ▶ See what TCP/IP does, and discover why it is so pervasive.
- ▶ View the big picture: see how applications run atop TCP/IP and how it rides on Frame Relay which, in turn, rides on T-carriers.
- ▶ See where Asynchronous Transfer Mode fits into the mix, and how ATM may fit into your telecommunications plans.
- ▶ Be able to recognize the different forms of DSL and how they can work for you.
- ▶ Understand the capabilities and limitations of Gigabit and 10-Gigabit Ethernet.
- ▶ Understand the principles and practices that guide the successful implementation of Storage Area Networks.
- ▶ Practice your knowledge through in-class exercises.