Understanding Networking

From the TCP/IP Guide

Introduction to Networking

- What Is Networking?
- The Advantages (Benefits) of Networking
- The Disadvantages (Costs) of Networking

Fundamental Network Characteristics

- Protocols: What Are They, Anyway?
- Circuit Switching and Packet Switching Networks
- Connection-Oriented and Connectionless Protocols
- Messages: Packets, Frames, Datagrams and Cells
- Message Formatting: Headers, Payloads and Footers
- Message Addressing and Transmission Methods: Unicast, Broadcast and Multicast Messages
- Network Structural Models and Client/Server and Peer-to-Peer Networking

Backgrounder: Data Representation and the Mathematics of Computing

- Binary Information and Representation: Bits, Bytes, Nibbles, Octets and Characters
- Decimal, Binary, Octal and Hexadecimal Numbers
- Decimal, Binary, Octal and Hexadecimal Number Conversion
- Binary, Octal and Hexadecimal Arithmetic
- Boolean Logic and Logical Functions
- Bit Masking (Setting, Clearing and Inverting) Using Boolean Logical Functions

History of the OSI Reference Model

General Reference Model Issues

- The Benefits of Networking Models
- Why Understanding The OSI Reference Model Is Important To You
- How To Use The OSI Reference Model
- Comparing the OSI Reference Model to Network Architectures and Protocol Stacks

Key OSI Reference Model Concepts

- OSI Reference Model Networking Layers, Sublayers and Layer Groupings

- "N" Notation and Other OSI Model Layer Terminology
- Interfaces: Vertical (Adjacent Layer) Communication

- Protocols: Horizontal (Corresponding Layer) Communication
- Data Encapsulation, Protocol Data Units (PDUs) and Service Data Units (SDUs)
- Indirect Device Connection and Message Routing

Understanding The OSI Reference Model: An Analogy

OSI Reference Model Layers

- Physical Layer (Layer 1)
- Data Link Layer (Layer 2)
- Network Layer (Layer 3)
- Transport Layer (Layer 4)
- Session Layer (Layer 5)
- Presentation Layer (Layer 6)
- Application Layer (Layer 7)

Types and Sizes of Networks

- Local Area Networks (LANs), Wireless LANs (WLANs) and Wide Area Networks (WANs) and Variants (CANs, MANs and PANs)
- Segments, Networks, Subnetworks and Internetworks
- The Internet, Intranets and Extranets

Backgrounder: Data Representation and the Mathematics of Computing

- Binary Information and Representation: Bits, Bytes, Nibbles, Octets and Characters
- Decimal, Binary, Octal and Hexadecimal Numbers
- Decimal, Binary, Octal and Hexadecimal Number Conversion
- Binary, Octal and Hexadecimal Arithmetic
- Boolean Logic and Logical Functions
- Bit Masking (Setting, Clearing and Inverting) Using Boolean Logical Functions

OSI Reference Model Layer Mnemonics

OSI Reference Model Layer Summary

TCP/IP Protocol Suite and Architecture

- TCP/IP Overview and History
- TCP/IP Services and Client/Server Operation
- TCP/IP Architecture and the TCP/IP Model
- TCP/IP Protocols

Additional Topics

- Private Addressing

- Subnetting
- NAT
- IPv6

Other Sources

VLAN

- Cisco IOS Switching Services Configuration Guide, Routing Between VLANs Overview
- AlliedWare Plus™ OS, Overview of VLANs (Virtual LANs)
- Firewll.cx, The VLAN Concept - Introduction to VLANs

STP

- Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide, Release 4.1.x, Chapter 6, Configuring STP and RSTP
- Cisco, Understanding Rapid Spanning Tree Protocol (802.1w)

More on ICMP from the TCP/IP Guide

ICMP Concepts and General Operation

- ICMP Overview, History, Versions and Standards
- ICMP General Operation
- ICMP Message Classes, Types and Codes
- ICMP Message Creation and Processing Conventions and Rules
- ICMP Common Message Format and Data Encapsulation

More on OSPF from the TCP/IP Guide

Open Shortest Path First (OSPF)

- OSPF Overview, History, Standards and Versions
- OSPF Basic Topology and the Link State Database
- OSPF Hierarchical Topology, Areas and Router Roles
- OSPF Route Determination Using SPF Trees
- OSPF General Operation and Message Types
- OSPF Message Formats

More on EIGRP

- Enhanced Interior Gateway Routing Protocol (EIGRP) (TCP/IP Guide)

- Enhanced Interior Gateway Routing Protocol (EIGRP) Informational RFC Frequently Asked Questions (Cisco)
- Implementing EIGRP (Cisco Press)
- Fundamental EIGRP Concepts (Cisco Press)

More on BGP from the TCP/IP Guide

BGP Fundamentals and General Operation

- BGP Overview, History, Standards and Versions
- BGP Topology, Speakers, Border Routers and Neighbor Relationships (Internal and External Peers)
- BGP Autonomous System Types, Traffic Flows and Routing Policies
- BGP Route Storage and Advertisement, and BGP Routing Information Bases (RIBs)
- BGP Path Attributes and Algorithm Overview
- BGP Route Determination and the BGP Decision Process
- BGP General Operation and Messaging

BGP Detailed Messaging, Operation and Message Formats

- BGP Message Generation and Transport, and General Message Format
- BGP Connection Establishment: Open Messages
- BGP Route Information Exchange: Update Messages
- BGP Connectivity Maintenance: Keepalive Messages
- BGP Error Reporting: Notification Messages

Using Netstat

- How to See What Web Sites Your Computer is Secretly Connecting To, Lori Kaufman, How-To Geek
- Using the Netstat Command to Monitor Network Traffic, Sean Wilkins, Petri IT Knowledgebase
- Netstat tips and tricks for Windows Server admins, Rick Vanover, TechRepublic
- Netstat, Microsoft TechNet
- Netstat, Mac OS X version 10.9 Manual

The TCP/IP Guide: TCP/IP Dynamic Host Configuration Protocol (DHCP)

- DHCP Overview, Motivation, History and Standards
- DHCP Address Assignment and Dynamic Address Allocation and Management
- DHCP Configuration and Operation
- DHCP Messaging, Message Types and Formats

- DHCP Client/Server Implementation, Features and Issues
- DHCP For IP Version 6 (DHCPv6)

The TCP/IP Guide: DNS

- DNS Overview, Functions and Characteristics
- DNS Name Space, Architecture and Terminology
- DNS Name Registration, Public Administration, Zones and Authorities
- DNS Name Servers and Name Resolution
- DNS Changes To Support IP Version 6

Additional Readings

DNS Root Servers

- Why There Are Only 13 DNS Root Name Servers, Bradley Mitchell, Lifewire
- Why 13 DNS root servers?, Miek Gieben

Hosts File

- Hosts file hijacks, Pieter Arntz, Malwarebytes
- 6 Surprising Uses for the Windows Hosts File, Chris Hoffman, MakeUseOf
- how to make the internet not suck (as much), Dan Pollock, someonewhocares.org
- The Hosts File and what it can do for you, Lawrence Abrams, BleepingComputer
- What are these 127.0.0.1 entries in my system hosts file?, Leo A. Notenboom, Ask Leo!
- How to effectively prevent Malware by using a HOSTS file, Shanmuga, Malware Help

Google Public DNS

- Google Public DNS: Get Started, Google Developers Guide
- How to Switch to OpenDNS or Google DNS to Speed Up Web Browsing, Taylor Gibb, How-To Geek
- Google DNS: 8.8.8.8 and 8.8.4.4. Benefits and how to use, Tunecomp

More About Firewall Techniques

In addition to firewalls, organizations can deploy a DMZ (demilitarized zone) to physically separate servers that the public should access from the servers that the public should not access.

Network Security First-Step: Firewalls, Donald Stoddard, Thomas M. Thomas, Cisco Press

DMZ (computing), Wikipedia

Virtual DMZs in the Cloud, Dejan Lukan, InfoSec Institute

Firewall DMZ Zone, Firewall.cx

More About IDSs and IPSs

IDFAQ: How do you deploy network based Intrusion Detection Systems in a switched network?, Brian W. Laing, The SANS Institute

Using IDS Sensors in Switched Networks, A. Lukatsky, flylib.com

SPAN Port or TAP? CSO Beware, Tim O'Neill, LoveMyTool.com

Implementing Networks Taps with Network Intrusion Detection Systems, Nathan Einwechter, Symantec

SPAN Port Or TAP? White Paper, Gigamon (pdf)

Port Mirror vs Network Tap, ntop

How to capture traffic? (SPAN vs TAP), Boris Rogier, PerformanceVision

Intrusion Detection System (IDS) Deployments with Network, ©Ixia/Net Optics, Network Performance Channel GmbH

Snort: Port Mirroring, OpenManiak

Switch Port Mirroring, SecurityWizardry

Finding Device Addresses and sending Network Traffic

Use one of these links to look up your own network information.

How to Find Any Device's IP Address, MAC Address, and Other Network Connection Details, How-To Geek

6 Ways to find the MAC address of any network card, in Windows, Ciprian Adrian Rusen, Digital Citizen

Then, using one or more of these links, send traffic from your computer to another device on your network, as well as a device on a different network.

How to Ping a Computer or a Web Site, Bradley Mitchell, Lifewire

How to Ping an IP Address, wikiHow

How to run a ping test, iiNet

You can also go to this site and find out the manufacturer of your network card through your MAC address.

OUI Lookup Tool, Wireshark

When you're finished, complete the survey and word clouds with what you were able to find out.

Take one or all of these phishing recognition tests to see how well you can spot fraudulent emails from legitimate ones.

- SonicWall Phishing IQ Test, SonicWall
- Phishing Quiz: Think you can Outsmart Internet Scammers?, Cisco
- Can you spot a fake email? Take our phishing IQ test, Kim Komando