# CCNA EXPLORATION V4.0
# ACCESSING THE WAN
# INSTRUCTOR REFERENCE GUIDE

## COMPARISON OF NEW CURRICULA WITH EXISTING CURRICULA

**Prepared by**
**Cisco Learning Institute**

**March 24, 2008**

## Accessing the WAN Summary

New CCNA curriculum has been created to improve student experience, improve quality, and increase flexibility.

## Accessing the WAN Course Outline

Following is the outline for this new course with indications as to which topics contain new content. Note: P-New means that the original subject matter has been enhanced and/or there is additional subject matter in the section.

| Course Outline | | | | New / Existing Content |
|---|---|---|---|---|
| **1.0** | | | **Introduction to WANs** | |
| | 1.1 | | Providing Integrated Services to the Enterprise | |
| | | 1.1.1 | Introducing Wide Area Networks (WANs) | P-New, 2.1.1 |
| | | 1.1.2 | The Evolving Enterprise | P-New, 2.3.3 |
| | | 1.1.3 | The Evolving Network Model | P-New, 2.3.4, 2.3.5 |
| | 1.2 | | WAN Technology Concepts | |
| | | 1.2.1 | WAN Technology Overview | 2.1.3 |
| | | 1.2.2 | WAN Physical Layer Concepts | 2.1.1-2.1.3 |
| | | 1.2.3 | WAN Data Link Layer Concepts | 2.1.2-2.1.4, 2.1.6 |
| | | 1.2.4 | WAN Switching Concepts | 2.1.5 |
| | 1.3 | | WAN Connection Options | |
| | | 1.3.1 | WAN Link Connection Options | P-New, 2.1.6 |
| | | 1.3.2 | Dedicated Connection Link Options | 2.2.3 |
| | | 1.3.3 | Circuit Switched Connection Options | 2.2.1, 2.2.2 |
| | | 1.3.4 | Packet Switched Connection Options | 2.2.4-2.2.6 |
| | | 1.3.5 | Internet Connection Options | P-New, 2.1.6, 2.2.7, 2.2.8 |
| **2.0** | | | **PPP** | |
| | 2.1 | | Serial Point-to-Point Links | |
| | | 2.1.1 | Introducing Serial Communications | P-New, 3.1.1 |
| | | 2.1.2 | TDM | 3.1.2 |
| | | 2.1.3 | Demarcation Point | 3.1.3 |
| | | 2.1.4 | DTE and DCE | 3.1.4 |
| | | 2.1.5 | HDLC Encapsulation | 3.1.5 |
| | | 2.1.6 | Configuring HDLC Encapsulation | 3.1.6 |
| | | 2.1.7 | Troubleshooting a Serial Interface | 3.1.7 |
| | 2.2 | | PPP Concepts | |
| | | 2.2.1 | Introducing PPP | 3.2.1 |
| | | 2.2.2 | PPP Layered Architecture | 3.2.1 |
| | | 2.2.3 | PPP Frame Structure | 3.2.1 |
| | | 2.2.4 | Establishing a PPP Session | 3.2.2 |
| | | 2.2.5 | Establishing a Link with LCP | 3.2.2-3.2.5 |
| | | 2.2.6 | NCP Explained | P-New, 3.2.2 |
| | 2.3 | | Configuring PPP | |
| | | 2.3.1 | PPP Configuration Options | 3.3.1 |
| | | 2.3.2 | PPP Configuration Commands | 3.3.2 |

| Course Outline | | | | New / Existing Content |
|---|---|---|---|---|
| | | 2.3.3 | Verifying a Serial PPP Encapsulation Configuration | 3.3.4 |
| | | 2.3.4 | Troubleshooting PPP Encapsulation | P-New, 3.3.5 |
| | 2.4 | | Configuring PPP with Authentication | |
| | | 2.4.1 | PPP Authentication Protocols | 3.2.3 |
| | | 2.4.2 | Password Authentication Protocol (PAP) | 3.2.4 |
| | | 2.4.3 | Challenge Handshake Authentication Protocol (CHAP) | 3.2.5 |
| | | 2.4.4 | PPP Encapsulation and Authentication Process | 3.2.6 |
| | | 2.4.5 | Configuring PPP with Authentication | 3.2.6 |
| | | 2.4.6 | Troubleshooting a PPP Configuration with Authentication | 3.3.5 |
| **3.0** | | | **Frame Relay** | |
| | 3.1 | | Basic Frame Relay Concepts | |
| | | 3.1.1 | Introducing Frame Relay | P-New, 5.1.1, 5.1.2 |
| | | 3.1.2 | Virtual Circuits | P-New, 5.1.2 |
| | | 3.1.3 | Frame Relay Encapsulation | 5.1.3 |
| | | 3.1.4 | Frame Relay Topologies | P-New, 5.1.5 |
| | | 3.1.5 | Frame Relay Address Mapping | P-New, 5.1.6, 5.1.7 |
| | 3.2 | | Configuring Frame Relay | |
| | | 3.2.1 | Configuring Basic Frame Relay | 5.2.1 |
| | | 3.2.2 | Configuring Static Frame Relay Maps | 5.2.2 |
| | 3.3 | | Advanced Frame Relay Concepts | |
| | | 3.3.1 | Solving Reachability Issues | 5.2.3, 5.2.4 |
| | | 3.3.2 | Paying for Frame Relay | NEW |
| | | 3.3.3 | Frame Relay Flow Control | 5.1.4 |
| | 3.4 | | Configuring Advanced Frame Relay | |
| | | 3.4.1 | Configuring Frame Relay Subinterfaces | 5.2.5, 5.2.4 |
| | | 3.4.2 | Verifying Frame Relay Operation | 5.2.6 |
| | | 3.4.3 | Troubleshooting Frame Relay Configuration | 5.2.7 |
| **4.0** | | | **Network Security** | |
| | 4.1 | | Introduction to Network Security | |
| | | 4.1.1 | Why is Network Security Important? | NEW |
| | | 4.1.2 | Common Security Threats | NEW |
| | | 4.1.3 | Types of Network Attacks | NEW |
| | | 4.1.4 | General Mitigation Techniques | NEW |
| | | 4.1.5 | The Network Security Wheel | NEW |
| | | 4.1.6 | The Enterprise Security Policy | NEW |
| | 4.2 | | Securing Cisco Routers | |
| | | 4.2.1 | Router Security Issues | NEW |
| | | 4.2.2 | Applying Cisco IOS Security Features to Routers | NEW |
| | | 4.2.3 | Manage Router Security | NEW |
| | | 4.2.4 | Securing Remote Administrative Access to Routers | NEW |

| Course Outline | | | | New / Existing Content |
|---|---|---|---|---|
| | | 4.2.5 | Logging Router Activity | 6.2.9 |
| | 4.3 | | Secure Router Network Services | |
| | | 4.3.1 | Vulnerable Router Services and Interfaces | NEW |
| | | 4.3.2 | Management Service Vulnerabilities | NEW |
| | | 4.3.3 | Securing Routing Protocols | NEW |
| | | 4.3.4 | Locking Down Your Router with Cisco Auto Secure | NEW |
| | 4.4 | | Using Cisco SDM | |
| | | 4.4.1 | Cisco SDM Overview | NEW |
| | | 4.4.2 | Configuring Your Router to Support Cisco SDM | NEW |
| | | 4.4.3 | Starting Cisco SDM | NEW |
| | | 4.4.4 | The Cisco SDM Interface | NEW |
| | | 4.4.5 | Cisco SDM Wizards | NEW |
| | | 4.4.6 | Locking Down a Router with Cisco SDM | NEW |
| | 4.5 | | Secure Router Management | |
| | | 4.5.1 | Maintaining Cisco IOS Software Images | NEW |
| | | 4.5.2 | Managing Cisco IOS Images | NEW |
| | | 4.5.3 | Managing Cisco IOS Images | NEW |
| | | 4.5.4 | Backing up and Upgrading Software Images | NEW |
| | | 4.5.5 | Recovering Software Images | NEW |
| | | 4.5.6 | Troubleshooting Cisco IOS Configurations | NEW |
| | | 4.5.7 | Recovering a Lost Router Password | NEW |
| **5.0** | | | **ACLs** | |
| | 5.1 | | Using ACLs to Secure Networks | |
| | | 5.1.1 | A TCP Conversation | NEW |
| | | 5.1.2 | Packet Filtering | NEW |
| | | 5.1.3 | What is an ACL? | NEW |
| | | 5.1.4 | ACL Operation | NEW |
| | | 5.1.5 | Types of Cisco ACLs | NEW |
| | | 5.1.6 | How a Standard ACL Works | NEW |
| | | 5.1.7 | Numbering and Naming ACLs | NEW |
| | | 5.1.8 | Where to Place ACLs | NEW |
| | | 5.1.9 | General Guidelines for Creating ACLs | NEW |
| | 5.2 | | Configuring Standard ACLs | |
| | | 5.2.1 | Entering Criteria Statements | NEW |
| | | 5.2.2 | Configuring a Standard ACL | NEW |
| | | 5.2.3 | ACL Wildcard Masking | NEW |
| | | 5.2.4 | Applying Standard ACLs to Interfaces | NEW |
| | | 5.2.5 | Editing Numbered ACLs | NEW |
| | | 5.2.6 | Creating Standard Named ACLs | NEW |
| | | 5.2.7 | Monitoring and Verifying ACLs | NEW |
| | | 5.2.8 | Editing Named ACLs | NEW |
| | 5.3 | | Configuring Extended ACLs | |

| Course Outline | | | | New / Existing Content |
|---|---|---|---|---|
| | | 5.3.1 | Extended ACLs | NEW |
| | | 5.3.2 | Configuring Extended ACLs | NEW |
| | | 5.3.3 | Applying Extended ACLs to Interfaces | NEW |
| | | 5.3.4 | Creating Named Extended ACLs | NEW |
| | 5.4 | | Configure Complex ACLs | |
| | | 5.4.1 | What are Complex ACLs? | NEW |
| | | 5.4.2 | Dynamic ACLs | NEW |
| | | 5.4.3 | Reflexive ACLs | NEW |
| | | 5.4.4 | Time-based ACLs | NEW |
| | | 5.4.5 | Troubleshooting Common ACL Errors | NEW |
| **6.0** | | | **Teleworker Services** | |
| | 6.1 | | Business Requirements for Teleworker Services | |
| | | 6.1.1 | The Business Requirements for Teleworker Services | NEW |
| | | 6.1.2 | The Teleworker Solution | NEW |
| | 6.2 | | Broadband Services | |
| | | 6.2.1 | Connecting Teleworkers to the WAN | P-New, 2.1.2 |
| | | 6.2.2 | Cable | P-New, 2.2.8 |
| | | 6.2.3 | DSL | P-New, 2.2.7 |
| | | 6.2.4 | Broadband Wireless | NEW |
| | 6.3 | | VPN Technology | |
| | | 6.3.1 | VPNs and Their Benefits | NEW |
| | | 6.3.2 | Types of VPNs | NEW |
| | | 6.3.3 | VPN Components | NEW |
| | | 6.3.4 | Characteristics of Secure VPNs | NEW |
| | | 6.3.5 | VPN Tunneling | NEW |
| | | 6.3.6 | VPN Data Integrity | NEW |
| | | 6.3.7 | IPsec Security Protocols | NEW |
| **7.0** | | | **IP Addressing Services** | |
| | 7.1 | | DHCP | |
| | | 7.1.1 | Introducing DHCP | P-New, 1.2.1, 1.2.3 |
| | | 7.1.2 | DHCP Operation | 1.2.1, 1.2.3, 1.2.4 |
| | | 7.1.3 | BOOTP and DHCP | P-New, 1.2.2 |
| | | 7.1.4 | Configuring a DHCP Server | 1.2.5, 1.2.6 |
| | | 7.1.5 | Configuring a DHCP Client | P-New, 1.2.4 |
| | | 7.1.6 | DHCP Relay | 1.2.8 |
| | | 7.1.7 | Configuring a DHCP Server Using SDM | NEW |
| | | 7.1.8 | Troubleshooting DHCP | P-New, 1.2.7 |
| | 7.2 | | Scaling Networks with NAT | |
| | | 7.2.1 | Private and Public IP Addressing | P-New, 1.1.1 |
| | | 7.2.2 | What is NAT? | 1.1.2-1.1.4 |
| | | 7.2.3 | Benefits and Drawbacks of Using NAT | 1.1.3, 1.1.7 |
| | | 7.2.4 | Configuring Static NAT | 1.1.4 |

| Course Outline | | | | New / Existing Content |
|---|---|---|---|---|
| | | 7.2.5 | Configuring Dynamic NAT | 1.1.4 |
| | | 7.2.6 | Configuring NAT Overload | 1.1.4 |
| | | 7.2.7 | Configuring Port Forwarding | NEW |
| | | 7.2.8 | Verifying and Troubleshooting NAT Configurations | P-New, 1.1.6 |
| | 7.3 | | IPv6 | |
| | | 7.3.1 | Reasons for Using IPv6 | NEW |
| | | 7.3.2 | IPv6 Addressing | NEW |
| | | 7.3.3 | IPv6 Transition Strategies | NEW |
| | | 7.3.4 | Cisco IOS Dual Stack | NEW |
| | | 7.3.5 | IPv6 Tunneling | NEW |
| | | 7.3.6 | Routing Considerations with IPv6 | NEW |
| | | 7.3.7 | Configuring IPv6 Addresses | NEW |
| | | 7.3.8 | Configuring RIPng with IPv6 | NEW |
| | | 7.3.9 | Reasons for Using IPv6 | NEW |
| **8.0** | | | **Network Troubleshooting** | |
| | 8.1 | | Establishing the Network Performance Baseline | |
| | | 8.1.1 | Documenting Your Network | P-New, 6.2.1, 6.2.2, 6.2.9 |
| | | 8.1.2 | Documenting Your Network | NEW |
| | | 8.1.3 | Why is Establishing a Network Baseline Important? | P-New, 6.2.8 |
| | | 8.1.4 | Steps for Establishing a Network Baseline | P-New, 6.2.9 |
| | 8.2 | | Troubleshooting Methodologies and Tools | |
| | | 8.2.1 | A General Approach to Troubleshooting | NEW |
| | | 8.2.2 | Using Layered Models for Troubleshooting | NEW |
| | | 8.2.3 | General Troubleshooting Procedures | NEW |
| | | 8.2.4 | Troubleshooting Methods | NEW |
| | | 8.2.5 | Gathering Symptoms | NEW |
| | | 8.2.6 | Troubleshooting Tools | P-New, 6.2.1, 6.2.4-6.2.6, 6.2.8, 6.2.9 |
| | 8.3 | | Common WAN Implementation Issues | |
| | | 8.3.1 | WAN Communications | 2.1.2, 2.1.6, 2.3.1 |
| | | 8.3.2 | Steps in WAN Design | P-New, 2.3.1-2.3.3 |
| | | 8.3.3 | WAN Traffic Considerations | P-New, 2.3.2, 2.3.3 |
| | | 8.3.4 | WAN Topology Considerations | 2.3.3 |
| | | 8.3.5 | WAN Bandwidth Considerations | 2.3.2, 2.3.3 |
| | | 8.3.6 | Common WAN Implementation Issues | 2.3.2 |
| | | 8.3.7 | Case Study: WAN Troubleshooting from an ISP's Perspective | NEW |
| | 8.4 | | Network Troubleshooting | |
| | | 8.4.1 | Interpreting Network Diagrams to Identify Problems | NEW |
| | | 8.4.2 | Physical Layer Troubleshooting | NEW |
| | | 8.4.3 | Data Link Layer Troubleshooting | P-New, 3.1.7, |

| Course Outline | | | | New/ Existing Content |
|---|---|---|---|---|
| | | | | 3.3.4, 3.3.5, 5.2.6, 5.2.7 |
| | | 8.4.4 | Network Layer Troubleshooting | NEW |
| | | 8.4.5 | Transport Layer Troubleshooting | NEW |
| | | 8.4.6 | Application Layer Troubleshooting | NEW |

## Accessing the WAN Summary of Skills and Equipment Changes:

### NEW SKILLS REQUIRED

Following is a list of the new skills that shall be required for the Accessing the WAN course:

- Configure router security with Cisco IOS and SDM.
- Configuration of remote access to routers using VPN.
- Advanced ACL configuration.
- IP6 configuration.
- Enterprise troubleshooting using Cisco's layered model.

### EQUIPMENT REQUIRED

**Academies adopting all CCNA Exploration courses – The minimum required equipment bundle for assured compatibility with all labs**:

In order to be able to implement the different topologies that are used in the lab exercises of the CCNA curricula, Academies teaching the four courses of either CCNA Exploration and/or CCNA Discovery require as a minimum the following equipment:

- 3 Cisco 1841 routers with Base IP IOS
- 3 2960 switches
- 2 Linksys wireless routers (Linksys WRT150N is preferred, but other models like the WRT54G, WRT300N, and WRT350N are alternatives) or SOHO equivalent

Note: The routers and switches in this equipment bundle can be substituted by other models of Cisco routers and switches with equal or higher specifications. Older equipment may be used as a substitute in some cases, but compatibility with labs is not guaranteed.

**Additional Lab Equipment Required:**

In addition to the networking equipment specified above, the lab topologies of CCNA Exploration may require the use of some or all of the following equipment and accessories:

- 1 PC acting as an Application Server
- A minimum of 2 desktop/laptop PCs acting as clients
- NIC Cards for the PC server and PC clients
- 2 Wireless LAN Adapters for the client PCs
- Ethernet cables and Serial Cables
- Cable-making and testing equipment

### IOS Option:

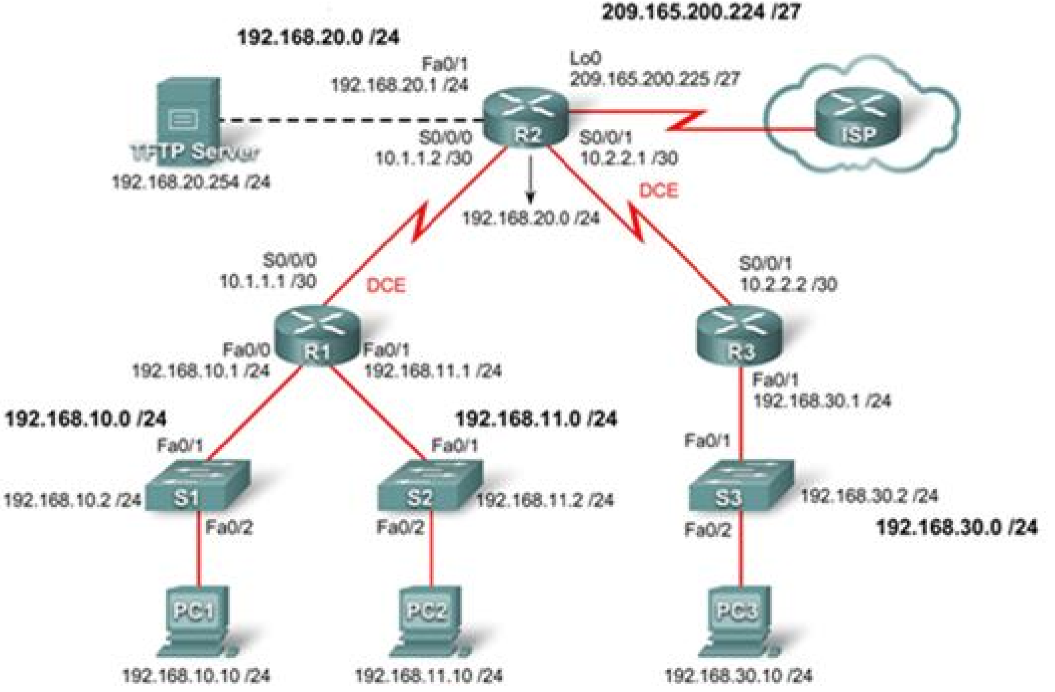
In order to keep equipment investment to a minimum, the Product Development team designed all lab exercises for CCNA Exploration using the BASE IP IOS 12.4. For those Academies that wish to drill deeper into some of the routing functionalities, Cisco recommends an upgrade of the BASE IP IOS to the Advanced Services IOS. In addition to the software itself, this upgrade requires additional DRAM and Flash memories for the 1841 Routers.

### Mounting Rack Accessories:

The 1841 is a desktop router. Academies that prefer to install lab equipment in standard 19" racks can use the optional Rack Kit for the 1841.

### Topologies:

**CCNA Exploration: Accessing the WAN**



## Summary of Changes:

The CCNA Exploration: Accessing the WAN curriculum has some pedagogical changes that have been applied to make the learning process more effective. The changes include the following:

- Access Control Lists have moved from semester 2 and are more advanced.
- ISDN has been removed.
- Work stations and servers have been removed.
- Network Security has been added.
- Tele-worker services and remote access security have been added.
- IP6 configuration has been added.
- Enterprise troubleshooting has been added.
- Converged network services has been added.