



NLI's
Cisco® CCIE
Security Lab Guide

1ST EDITION

John Kaberna
CCIE #7146

Ray Fung
CCIE #6832

About the Author

John Kaberna is a dual Cisco Certified Internetwork Expert, CCIE #7146 (Routing/Switching and Security). John also holds the CCNP, CCDP, and CSS 1 certifications. He is the President and principal consultant for Network Consultants Group, Inc. based in San Francisco, CA. He has more than 6 years experience in Cisco networking and security including planning, designing, implementing, and troubleshooting large multiprotocol networks. John is currently designing and implementing a large retail network and is responsible for the security, performance, and management of their entire network. He also recently completed several major contracts for the U.S. Navy as a Cisco consultant and trainer. He also writes Cisco training material and is currently teaching CCIE courses for Network Learning, Inc.

Raymond Fung is a triple Cisco Certified Internetwork Expert #6832, holding designations in Routing/Switching, Security, and Communications/Services. He specializes in designing and troubleshooting service-provider and large-enterprise networks. He graduated magna cum laude with two engineering degrees from University of California, Berkeley. He is currently writing Cisco training materials for the upcoming Voice Over IP course.

Table of Contents

SECTION I LAYER 2 TECHNOLOGIES

CHAPTER 1: FRAME-RELAY

INTERFACE TYPES

Physical interfaces
Point-to-Point subinterfaces
Point-to-Multipoint subinterfaces

INVERSE ARP
FRAME MAPS
INTERFACE DLCI
SPLIT HORIZON
LMI TYPES
FRAME SWITCHING
TYPICAL GOTCHAS!

CHAPTER 2: ATM

TERMS
RFC 2684 versus RFC 2225
VCD, VPI, and VCI
ILMI and QSAAL
PVC CONFIGURATION
Subinterfaces
Autodiscovery
Map-group and map-lists
“New” way
Inverse ARP
SVC CONFIGURATION
TYPICAL GOTCHAS!

CHAPTER 3: ISDN

MINIMUM CONFIGURATION
ISDN Switch Type
Service Profile Identifier (SPID)
Dialer-list
Dialer-group
IP Address
Dial String

ADVANCED CONFIGURATIONS

Dialer-map
Idle Timeout
Fast Idle
HDLC
PPP
Multilink
Callback
Unidirectional authentication
Dial Backup (interface failure)

DIALER PROFILES

Example 1 – Multiple next hop routers
Example 2 – Changing the pool-member priority, minimum and maximum channels

Example 3 – Map classes

ISDN AND ROUTING PROTOCOLS

*Floating static routes**OSPF demand circuit**Dialer Watch**Snapshot routing*

TYPICAL GOTCHAS!

CHAPTER 4: BRIDGING

TRANSPARENT BRIDGING (TB)

INTEGRATED ROUTING AND BRIDGING (IRB)

CONCURRENT ROUTING AND BRIDGING (CRB)

TYPICAL GOTCHAS!

CHAPTER 5: CATALYST 3550 SWITCHING

SPANNING TREE (STA)

Spanning Tree Configuration

VIRTUAL LAN'S (VLAN)

VLAN Configuration

TRUNKING

Trunk Mode

ETHERCHANNEL

VLAN TRUNKING PROTOCOL (VTP)

TYPICAL GOTCHAS!

SECTION II LAYER 3 ROUTING PROTOCOLS**CHAPTER 6: GENERAL ROUTING**

NETWORK COMMAND

PASSIVE INTERFACE

SPLIT HORIZON

DISTANCE

TYPICAL GOTCHAS!

CHAPTER 7: OPEN SHORTAGE PATH FIRST

OSPF AREAS TYPES

PEER RELATIONSHIPS

AREA 0

BASIC OSPF CONFIGURATION

FRAME-RELAY AND OSPF

OSPF over Frame-Relay Configuration

DESIGNATED AND BACKUP DESIGNATED ROUTER ELECTIONS

LOOPBACKS

ROUTER ID

VIRTUAL LINKS

OSPF AUTHENTICATION

*Configuring OSPF clear-text authentication**Configuring OSPF MD5 authentication**Configuring OSPF Virtual-link Clear-Text Authentication**Configuring OSPF Virtual-link MD5 authentication*

TYPICAL GOTCHAS

CHAPTER 8: BORDER GATEWAY PROTOCOL (BGP)

BGP PEERS*Internal BGP (IBGP)**External BGP (EBGP)***BASIC BGP CONFIGURATION****SYNCHRONIZATION****NEXT-HOP-SELF****TRANSIT AS***Example 1 – Basic filters**Example 2 – Filters with ip as-path command**Example 3 – Communities***MD5 AUTHENTICATION****EBGP MULTIHOP****BGP PATH SELECTION***Weight**Local Preference**AS Path Manipulation**Metric and MED's***ROUTE AGGREGATION AND AUTO SUMMARY***Configuring Aggregate routes and specific routes**Configuring Aggregate routes without more specific routes***ROUTE REFLECTORS****CONFEDERATIONS****BGP PEER GROUPS****ROUTE DAMPENING****SOFT RECONFIGURATION***Outbound Soft Reconfiguration**Inbound Soft Reconfiguration***TYPICAL GOTCHAS!****CHAPTER 9: EIGRP****FEATURES OF EIGRP****TYPES OF SUCCESSORS****TABLES***Choosing routes***BASIC EIGRP CONFIGURATION****MANIPULATING ROUTES***Adjusting EIGRP Metrics**Manipulating Default Metrics**Auto Summarization**Manual Summarization**Default Routing**Stub Routing**Unequal Cost Load Balancing**Offset-Lists**Limiting EIGRP Bandwidth***STATIC NEIGHBORS****EIGRP TIMERS****TYPICAL GOTCHAS!****CHAPTER 10: RIP****BASIC RIP CONFIGURATION****ADJUSTING RIP TIMERS****UNICAST UPDATES****OFFSET LIST****SOURCE IP ADDRESS VALIDATION****INTERPACKET DELAY**

TYPICAL GOTCHAS!

CHAPTER 11: RIP VERSION 2

BASIC RIP VERSION 2 CONFIGURATION
AUTHENTICATION
 Key management
 Interface configuration
ROUTE SUMMARIZATION
DEMAND CIRCUIT
TYPICAL GOTCHAS!

CHAPTER 12: REDISTRIBUTION

REDISTRIBUTION ISSUES
BASIC REDISTRIBUTION
ADMINISTRATIVE DISTANCE ISSUE
ROUTING LOOP ISSUE
ROUTE MAPS
DISTRIBUTE LISTS
VLSM TO FLSM ISSUE
TYPICAL GOTCHAS!

SECTION III CISCO GENERAL SECURITY AND FIREWALLS

CHAPTER 13: CISCO ROUTER SECURITY

CISCO ROUTER SECURITY RECOMMENDATIONS
DISABLE UNNECESSARY SERVICES
 Cisco Discovery Protocol (CDP)
 Diagnostic Ports
 HTTP Server
 Finger
 DHCP and BOOTP Server
 ICMP Unreachables
 ICMP Redirect Messages
 Proxy Address Resolution Protocol (ARP)
PREVENTING MOST DENIAL OF SERVICE ATTACKS
 Ingress and Egress filtering
 Cisco Express Forwarding (CEF) and Unicast Reverse Path (RPF)
 TCP SYN Attacks
 TCP Intercept and Watch
 Committed Access Rate (CAR)
 Ping of Death
 Smurf attacks
ROUTER SELF PROTECTION
 Handling crash dumps
 Black Hole Routes
TYPICAL GOTCHAS!

CHAPTER 14: ACCESS LIST

General Rules of Access-Lists
 Recommendations
STANDARD
 Inbound blocking
 Outbound blocking
EXTENDED
COMMENTED ENTRIES

REFLEXIVE
TIME-BASED
DYNAMIC (LOCK AND KEY)
Configuration for 12.1.5T9
Configuration for other versions
ACL'S AND DEBUGS
TYPICAL GOTCHAS!

CHAPTER 15: IOS FIREWALL

TRAFFIC FILTERING
TRAFFIC INSPECTION
ALERTS AND AUDIT TRAILS
CONFIGURING CBAC
Configuring a basic two-port firewall
CBAC Session Timers and Threshold commands
Configuring IP Packet Fragmentation Inspection
Blocking Java applets
Permitting traffic through the IOS firewall
Network Address Translation (NAT)

CHAPTER 16: PIX FIREWALL

PIX FEATURES
BASIC PIX FIREWALL CONFIGURATION
Minimum PIX configuration
PERMITTING TRAFFIC THROUGH THE PIX
Static Translations
Conduit command
Access-list and access-group commands
ADVANCED FEATURES AND COMMANDS
Fixup command
Java applet filtering
ActiveX blocking
PIX Failover
Stateful Failover
Configuring Stateful Failover
Alias command
DHCP Server
DHCP Client
Outbound and Apply
RIP
Sysopt command
Mail Guard
DNS Guard
Service Reset Inbound
TYPICAL GOTCHAS!

SECTION IV VIRTUAL PRIVATE NETWORKS

CHAPTER 17: VPN OVERVIEW

IP SECURE (IPSEC)
DATA ENCRYPTION STANDARD (DES)
TRIPLE DES (3DES)
INTERNET KEY EXCHANGE (IKE)
TYPICAL GOTCHAS!

CHAPTER 18: VPN CONFIGURATION

EXAMPLE 1 - ROUTER TO ROUTER VPN USING 3DES AND IKE PRE-SHARED KEYS*Headquarters router configuration*[2](#)*Remote Site1 router configuration*[3](#)**EXAMPLE 2 - PIX TO PIX VPN WITH 3DES AND IKE PRE-SHARED KEYS**[4](#)*Headquarters Site PIX Configuration**Remote Site2 router configuration***EXAMPLE 3 – PIX TO TWO REMOTE ROUTERS WITH DES, 3DES, AND IKE PRE-SHARED KEYS***Headquarters PIX configuration*[7](#)*Remote Site1 router configuration*[7](#)*Remote Site2 router configuration*[8](#)**EXAMPLE 4 – PIX TO ROUTER WITH 3DES, IKE PRE-SHARED KEYS AND NAT**[8](#)*PIX IPSec Configuration with NAT**Router IPSec Configuration with NAT***EXAMPLE 5 – PIX TO ROUTER CONFIGURATION WITH DES AND MANUAL KEYS****HEADQUARTERS PIX CONFIGURATION***Remote site router configuration***VERIFICATION AND TROUBLESHOOTING****TYPICAL GOTCHAS!****CHAPTER 19: CERTIFICATE AUTHORITY****MICROSOFT CA CONFIGURATION***Setup and Install Certificate Authority on Windows 2000*[7](#)*Install Simple Certificate Enrollment Protocol*[7](#)*Setup the CA service*[0](#)**ROUTER AND PIX CONFIGURATION**[2](#)*Example 1 – Router to PIX VPN with 3DES and IKE RSA digital certificates***TYPICAL GOTCHAS!****CHAPTER 20: POINT-TO-POINT TUNNELING PROTOCOL****WINDOWS 98/NT/2000 CONFIGURATIONS FOR PPTP***Windows 98 Configuration**Windows 2000 Configuration**Windows NT 4.0 Configuration***PIX CONFIGURATION FOR PPTP****EXAMPLE 1 – PIX CONFIGURATION WITH LOCAL AUTHENTICATION AND NO ENCRYPTION****EXAMPLE 2 - PIX CONFIGURATION WITH LOCAL AUTHENTICATION AND ENCRYPTION****EXAMPLE 3 - PIX CONFIGURATION WITH RADIUS AUTHENTICATION AND ENCRYPTION****EXAMPLE 4 - ROUTER CONFIGURATION WITH RADIUS AUTHENTICATION AND ENCRYPTION****TROUBLESHOOTING PPTP CONNECTIONS****TYPICAL GOTCHAS!****CHAPTER 21: LAYER 2 TUNNELING PROTOCOL****L2TP CONFIGURATION***NAS/LAC Configuration**Tunnel Server/LNS Configuration***TYPICAL GOTCHAS!****CHAPTER 22: GRE TUNNELS AND IPSEC****GRE OVERVIEW****BASIC GRE CONFIGURATION****GRE AND ROUTING PROTOCOLS***Avoiding Recursive routing*

GRE OVER IPSEC
TYPICAL GOTCHAS![91](#)

SECTION V AAA, IDS AND NETWORK MANAGEMENT

CHAPTER 23: AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING

LOCAL AAA

Basic Local Authentication Configuration

Named Method Lists

Local Authorization Configuration

TERMINAL ACCESS CONTROLLER ACCESS CONTROL SYSTEM (TACACS) OVERVIEW

Basic TACACS+ Configuration

TACACS Login Authentication

TACACS+ PPP authentication

TACACS+ Authorization

AAA Server Group Configuration Tasks

TACACS+ Accounting

TACACS+ Accounting Configuration

REMOTE AUTHENTICATION DIAL-IN USER SERVICE (RADIUS)302

RADIUS Server Configuration

RADIUS AAA Configuration

PRIVILEGE LEVELS

TYPICAL GOTCHAS!

CHAPTER 24: INTRUSION DETECTION

IDS CONFIGURATION ON A ROUTER

Standalone configuration (without an IDS management application)

Configuration with an IDS management application

Additional IDS commands

IDS Verification

PIX IDS CONFIGURATION

Standalone configuration (without an IDS management application)

TYPICAL GOTCHAS!

CHAPTER 25: NETWORK MANAGEMENT

SECURE SHELL (SSH)

NETWORK TIME PROTOCOL (NTP)

Simple Network Management Protocol (SNMP)

Logging

TYPICAL GOTCHAS!

CATALYST 3550 SWITCHING

SPANNING TREE (STA)

STA was designed to allow for redundant paths between bridges while preventing loops. For example, two ports connect Bridge 1 and Bridge 2. In order to prevent a loop only one port is in use at a time. The port not in use is put into a status known as “blocking.” If there is a failure with the primary port, the blocked port will become active.

Each port in every bridge also is assigned a unique identifier, which is typically its own MAC address. Each switch port is associated with a path cost, which represents the cost of transmitting a frame onto a LAN through that port. Path costs have a default value depending on the type of port, but they can be changed manually by network administrators. Path costs on Catalyst switches are determined by interface type (Fast Ethernet, Gigabit Ethernet, Token-ring, FDDI, etc.).

The spanning-tree calculation occurs when the bridge is powered up and whenever a topology change is detected. The calculation involves sending configuration messages between bridges. These communication messages are known as bridge protocol data units, or BPDU's. BPDU's contain information identifying the bridge that is presumed to be the root and the distance from the sending bridge to the root bridge (root path cost). They also contain the bridge and port identifier of the sending bridge, as well as the age of the information.

Bridges exchange BPDU's at regular intervals (typically one to four seconds). If there is a failure of some sort and neighboring bridges stop receiving BPDU's they will initiate a spanning-tree recalculation.

SPANNING TREE CONFIGURATION

The Catalyst 3550 has many of the same STP features of the set-based switches with some enhancements and notable differences. Since the 3550 is IOS based, any changes made that you want to be permanent will need to be saved using `write mem` or `copy run start`. This rule also applies to the VLAN database covered later in this chapter.

DEFAULT STP VALUES

It may be helpful to know the default values for STP. Table 5.1 illustrates these values as of software version 12.1.4.

Table 5.1 STP Values

Feature	Default Setting
Switch priority	32768
STP and VLAN Port costs	1000 Mbps : 4 100 Mbps: 19 10 Mbps: 100
Port priority	128
Hello time	2 seconds
Forward-delay time	15 seconds
Maximum-aging time	20 seconds
Port Fast, BPDU Guard, UplinkFast, BackboneFast, Root guard	Disabled

DISABLE STP

Although unlikely, there may be situations where it is desirable to disable spanning-tree. If there is a loop in your layer 2 topology disabling spanning-tree will result in data being lost and severe network degradation. It is almost never recommended to disable spanning-tree. Use this command with caution.

To disable STP on a VLAN use the global command `no spanning-tree vlan <vlan_id>`.

ROOT SWITCH

The 3550 maintains a separate STP instance for each VLAN. So you will need to configure each VLAN individually that you want to make root. To make a switch root for a VLAN use the `spanning-tree vlan <vlan_id> root primary`. There are two optional parameters: diameter and hello-time. Diameter sets the maximum number of switches between any two hosts. This helps prevent loops by stopping a frame from endlessly traveling in a loop. Once the maximum number of switches is traversed the frame is dropped. Hello-time is a value between 1 and 10 seconds. It is simply how often a switch will send a “hello” frame to a switch that it has a trunk connection. The hello-time affects how quickly spanning-tree will detect a fault and use a new path.

```
Switch(config)# spanning-tree vlan 1 root primary diameter 3 hello-time 5
```

SECONDARY ROOT SWITCH

The secondary root switch is useful in situations where you have two switches that are typically in parallel (usually redundant core switches) where one should backup the other as the root bridge. The only difference between setting the primary and secondary root is the option after root.

```
Switch(config)# spanning-tree vlan 1 root secondary diameter 3 hello-time 5
```

PORT PRIORITY

When a switch has multiple paths it will put one in forwarding and the rest will be blocking. This is used for loop prevention. If all the interfaces have the same priority value (this will always happen unless you explicitly configure the port's value), then STP will use the lowest numbered interface (for example, it would use interface fastethernet 0/1 before fastethernet 0/2 assuming they were both connected to the root bridge) as the forwarding port. The only interfaces that can be configured for port priority are physical interfaces (not VLAN interfaces) and port-channel logical interfaces.

Note The default for IEEE STP is 128. The value can be from 0 to 255. The lower the number the higher the priority.

```
Switch(config)# interface fastethernet0/1  
Switch(config-if)# spanning-tree port-priority 1
```

PATH COST

By default, path costs are determined by the media speed of the interface. It is typically not necessary to change this value. Table 5-1 illustrates the path costs for each of the interface types available on the 3550.

The same basic rules apply to path cost as they do to port priority. If there are two paths from a switch to the root bridge, the first consideration is priority. If priority is equal, then path cost will be the deciding factor. If they are all equal, the switch will add the port priority and port ID of both interfaces. STP will then disable the link with the lowest value.

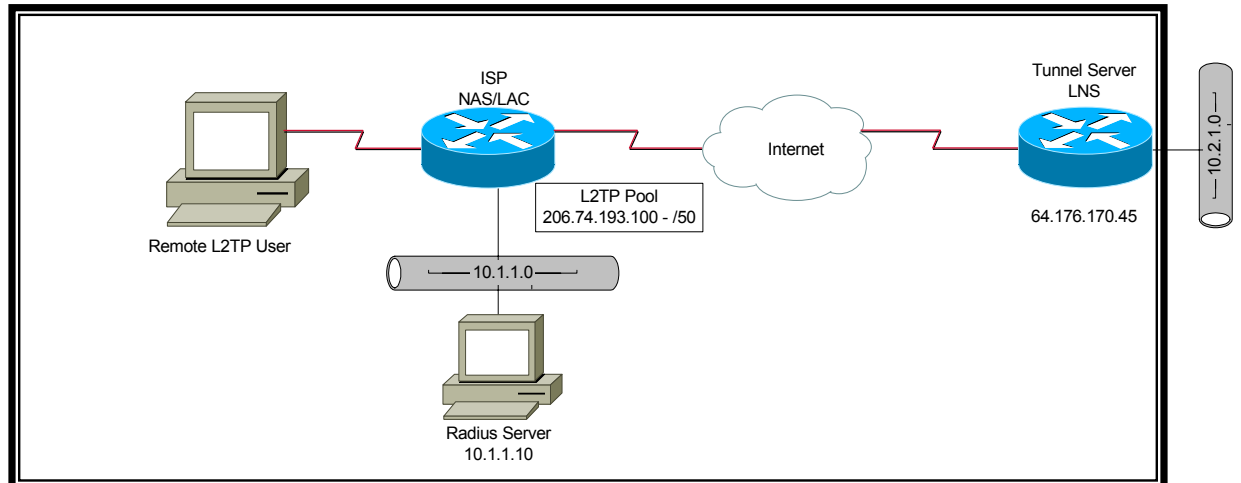
```
Switch(config)# interface fastethernet0/1  
Switch(config-if)# spanning-tree vlan 1 cost 10
```

LAYER 2 TUNNELING PROTOCOL

L2TP is a secure protocol used for connecting VPNs (Virtual Private Networks) over public lines such as the Internet. It is essentially a combination of two other secure communications protocols: PPTP and Cisco's Layer 2 Forwarding Protocol (L2F).

The layout for an L2TP VPN consists of a NAS and a tunnel server. The NAS is maintained by the ISP or provider. The NAS receives incoming calls for dial-in VPNs and places outgoing calls for dial-out VPNs. Normally when we think of a NAS we think of the access routers at a customer's site. The tunnel server terminates dial-in VPNs and initiates dial-out VPNs. This is usually maintained at the customer's site and can be managed by either the customer or the ISP. Typically, the customer will manage this device since this is the entrance point for VPN users into their private network.

Figure 21.1 Typical L2TP network setup



L2TP CONFIGURATION

Depending upon your role in an L2TP network, ISP or customer, your configurations may vary. The NAS is often referred to as the L2TP Access Concentrator (LAC). The tunnel server is often called the L2TP Network Server (LNS). All of our configurations will be based on NAS-initiated VPN's. NAS-initiated VPNs take place when users dial in to the ISP's NAS and establish a tunnel to the corporate network. From the NAS to the tunnel server, the connection is encrypted. However, the phone line connection between the client's PC and the ISP's NAS is not encrypted. This is generally not considered a high security risk, as is the Internet.

NAS/LAC CONFIGURATION

Step 1 Enable basic AAA commands for user authentication. Our example uses RADIUS since most dialup implementations use RADIUS.

```
nas-rtr1(config)# aaa new-model
nas-rtr1(config)# aaa authentication login ppp radius local
nas-rtr1(config)# radius-server host 10.1.1.10
nas-rtr1(config)# radius-server key cisco
```

Step 2 Configure the local pool of IP addresses.

```
nas-rtr1(config)# ip local pool l2tp-pool 172.16.1.10 172.16.1.100
```

Step 3 Configure the interface that accepts PPP calls. These examples show two typical interface types and their configurations. Consult your ISDN PRI circuit provider for exact configuration parameters. The following are the most common configurations.

ISDN PRI INTERFACE

```
nas-rtr1(config)# isdn switch-type basic-ni
nas-rtr1(config)# controller t1 0
nas-rtr1(config-controller)# framing esf
nas-rtr1(config-controller)# linecode b8zs
nas-rtr1(config-controller)# clock source line
nas-rtr1(config-controller)# pri-group timeslots 1-24
```

MODEM CONFIGURATION WITH 32 INTERNAL MODEMS ON LINES 33-64

```
nas-rtr1(config)# line 33 64
nas-rtr1(config-line)# autoselect ppp
nas-rtr1(config-line)# autoselect during-login
nas-rtr1(config-line)# modem inout
```

Step 1 Enable VPDN on the NAS.

```
nas-rtr1(config)# vpdn enable
```

Step 2 Configure the tunnel username and password. The username is the OTHER router's hostname or local name. The password must be the same on both sides.

```
nas-rtr1(config)# username lns-rtr1 password secret
```

-OR-

Configure the VPDN group password and optional username. By default, the router will send its hostname as its username to the other router. If you want the router to send a username other than the hostname, use the optional command below.

```
nas-rtr1(config)# vpdn-group 1
nas-rtr1(config-vpdn)# l2tp tunnel password
```

The following command will send the username `nas` instead of `nas-rtr1`. This command is optional.

```
nas-rtr1(config-vpdn)# local name nas
```

Step 3 Configure the VPDN group parameters. The first command enables the NAS to accept incoming dial-up requests. The second command selects the protocol to be used (either `l2tp`, `l2f`, or any).

```
nas-rtr1(config-vpdn)# request-dialin
nas-rtr1(config-vpdn-req-in)# protocol l2tp
nas-rtr1(config-vpdn-req-in)# domain name cisco.com
```

Step 4 Configure the IP address of the tunnel server that the NAS will connect to. The `limit` and `priority` commands are optional. These commands set a limit of 50 connections for this VPDN group and set the priority to 10.

```
nas-rtr1(config-vpdn)# initiate-to-ip 64.176.170.45 limit 50 priority 10
```

TYPICAL GOTCHAS!

- Incorrect AAA configuration on NAS
- Access-dialin and request-dialin on the wrong routers
- Missing l2tp protocol command under access-dialin and request-dialin
- Misconfigured virtual template interface