Professor Messer

Professor Messer's Cisco CCENT/CCNA 100-105 ICND1 Course Notes

James "Professor" Messer

Professor Messer's
Cisco CCENT/CCNA
100-105 ICND1 Course Notes

James "Professor" Messer

http://www.ProfessorMesser.com

Professor Messer's Cisco CCENT/CCNA 100-105 ICND1 Course Notes
Written by James "Professor" Messer

http://www.ProfessorMesser.com

First Edition: March 2017

Trademark Acknowledgements

Warning and Disclaimer
This book is designed to provide information about the Cisco CCENT/CCNA 100-105 ICND1 certification exam. However, there may be typographical and/or content errors. Therefore, this book should serve only as a general guide and not as the ultimate source of subject information. The author shall have no liability or responsibility to any person or entity regarding any loss or damage incurred, or alleged to have incurred, directly or indirectly, by the information contained in this book.

Contents

Introduction

If you're in the Information Technology industry, then you know that Cisco certifications are some of the most accepted (and most difficult) certifications to earn. Cisco certifications range from a fundamental networking knowledge to the most advanced networking technologies today.

Cisco certification exams test you on the specifics of routers, switches, ports, protocols, and much more. I've created these Course Notes to help you through the details that you need to know for the exam. Best of luck with your studies!

- Professor Messer

The Cisco CCENT/CCNA Routing and Switching certification

Earning the Cisco Certified Network Assocate Routing and Switching (CCNA R&S) certification requires either the completion of two separate exams (the ICND1 100-105 and ICND2 200-105), or the completion of a single combined exam (the 200-125).

THE INTERCONNECTING CISCO NETWORK DEVICES 1 (ICND1) 100-105 EXAM

These ICND1 100-105 Course Notes focus on the content required to pass the first half of the CCNA R&S. Passing the ICND1 100-105 exam earns you the Cisco Certified Entry Networking Technician (CCENT) certification, so you can earn some credentials as you move halfway towards achieving your CCNA R&S certification.

Here's the breakdown of each technology section and the percentage of each topic on the 100-105 exam:

Section 1.0 - Network Fundamentals - 20%
Section 2.0 - LAN Switching Fundamentals - 26%
Section 3.0 - Routing Fundamentals - 25%
Section 4.0 - Infrastructure Services - 15%
Section 5.0 - Infrastructre Maintenance - 14%

How to use this book

Once you're comfortable with all of the sections in the official Cisco 100-105 exam objectives, you can use these notes as a consolidated summary of the most important topics. These Course Notes follow the same format and numbering scheme as the official exam objectives, so it should be easy to cross reference these notes with all of your other study materials.


Professor
Messer

Professor Messer's

Cisco CCENT/CCNA

100-105 ICND1 Course Notes

http://www.ProfessorMesser.com

The 100-105 Cisco ICND1 Exam

100-105 Exam Objectives

- 1.0 - Network Fundamentals (20%)
- 2.0 - LAN Switching Fundamentals (26%)
- 3.0 - Routing Fundamentals (25%)
- 4.0 - Infrastructure Services (15%)
- 5.0 - Infrastructure Maintenance (14%)

- Exam time: 90 minutes
- 45 to 55 questions
- Scoring ranges between 300 and 1,000 points
- Passing score is given at the beginning of the exam

Introduction to the Cisco CLI

How to connect

- Interface with IOS through a CLI
  - Command Line Interface
- Serial cable to a console interface
- Across the network
  - Telnet, SSH

Serial cable to a console interface

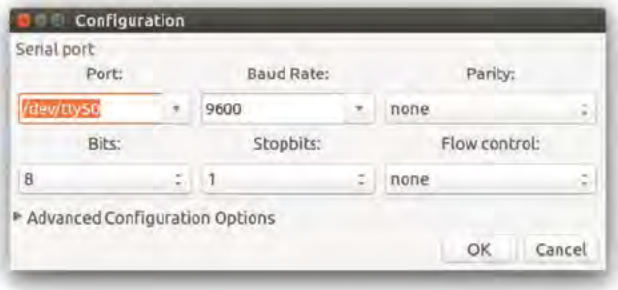
- From the computer
  - 9-pin serial connector or USB interface
- From the switch or router
  - 9-pin serial connector, RJ45 connector, USB interface
- You might need a USB to serial cable
  - And a set of adapters

IOS User Modes

- User EXEC mode
  - Execute commands as a normal user
  - No configuration changes allowed
- Privileged EXEC mode
  - "Enable mode"
- Initial login is to user mode
  - Use "`enable`" to enter privileged mode
  - And "`disable`" to leave

Serial interface settings

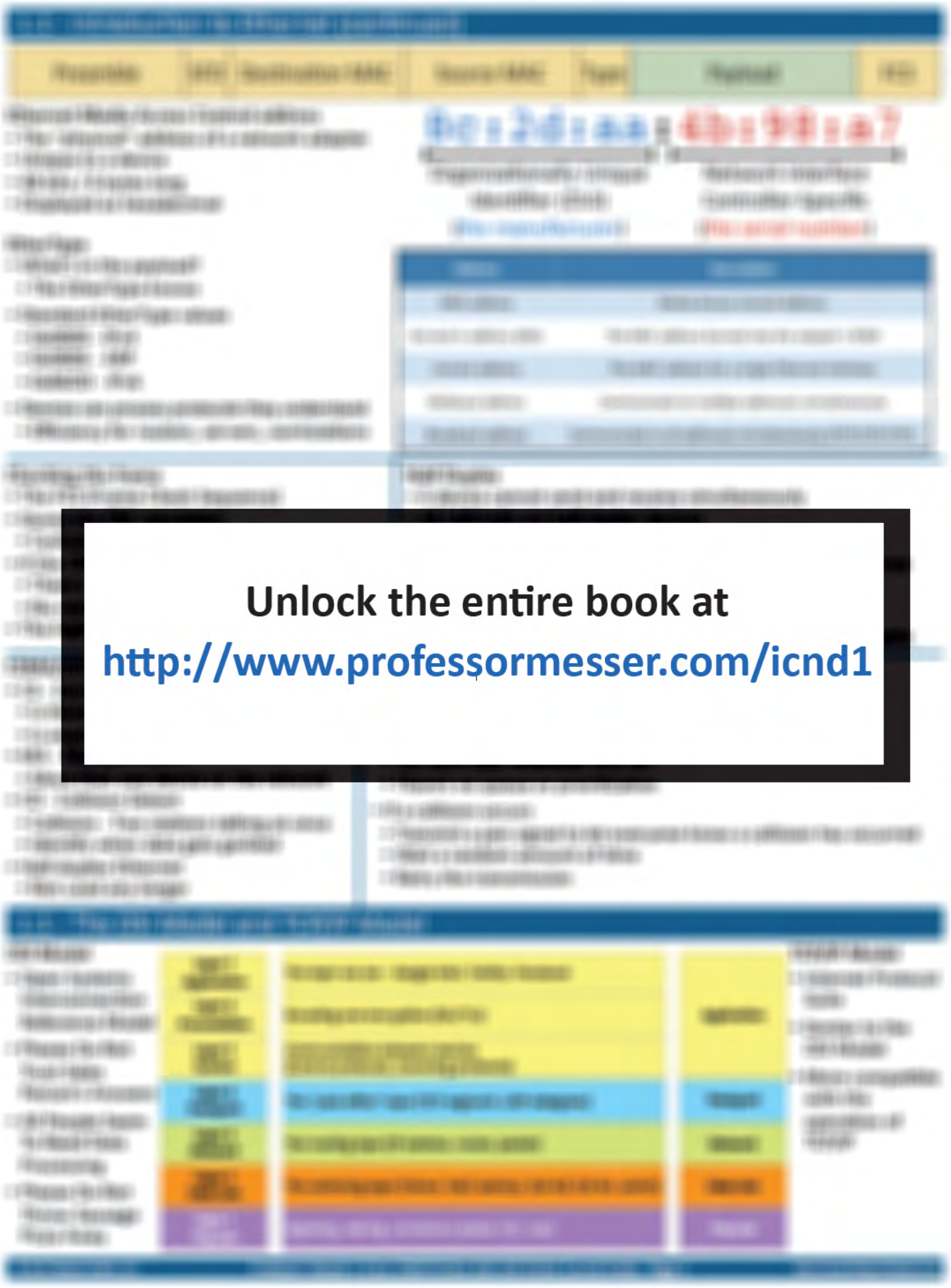
- This must match the settings on the other device
  - A mismatch results in a screen of scrambled text
- Port - The physical interface
- Baud rate - The speed of the data (9600 baud)
- Parity - None
- Data bits - 8
- Stop bits - 1
- Flow control - none



1.1 - Introduction to Ethernet - The Ethernet Frame

Field	Bytes	Description
Preamble	7	56 alternating ones and zeros used for synchronization (101010...)
SFD	1	Start Frame Delimiter - designates the end of the preamble (10101011)
Destination MAC Address	6	Ethernet MAC address of the destination device
Source MAC Address	6	Ethernet MAC address of the source device
EtherType	2	Describes the data contained the payload
Payload	46 - 1500	Layer 3 and higher data
FCS	4	Frame Check Sequence - CRC checksum of the frame

Preamble	SFD	Destination MAC	Source MAC	Type	Payload	FCS



Unlock the entire book at

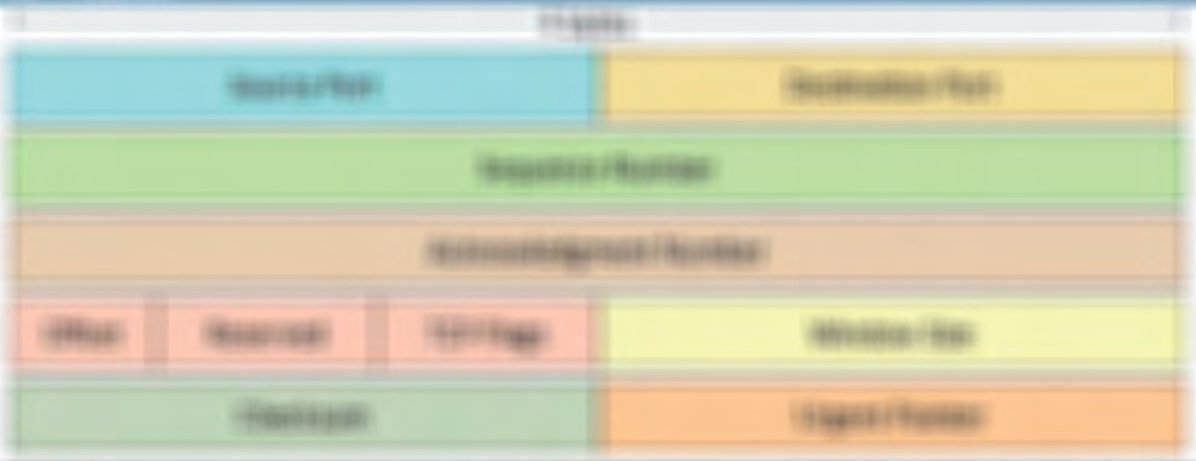
http://www.professormesser.com/icnd1

1.1.1 [illegible]

1.1.2 [illegible]

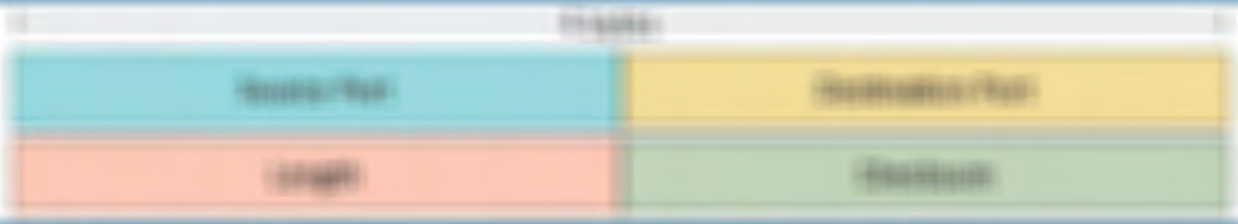
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]

1.1.3 [illegible]



[illegible]

[redacted]



[redacted]

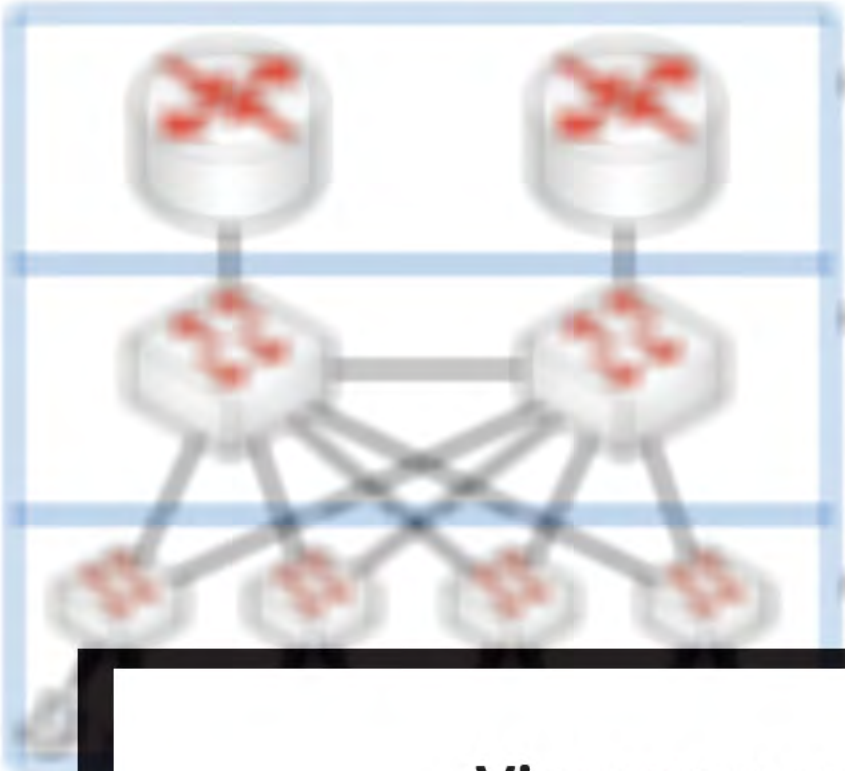
[redacted]

[redacted]

[redacted]

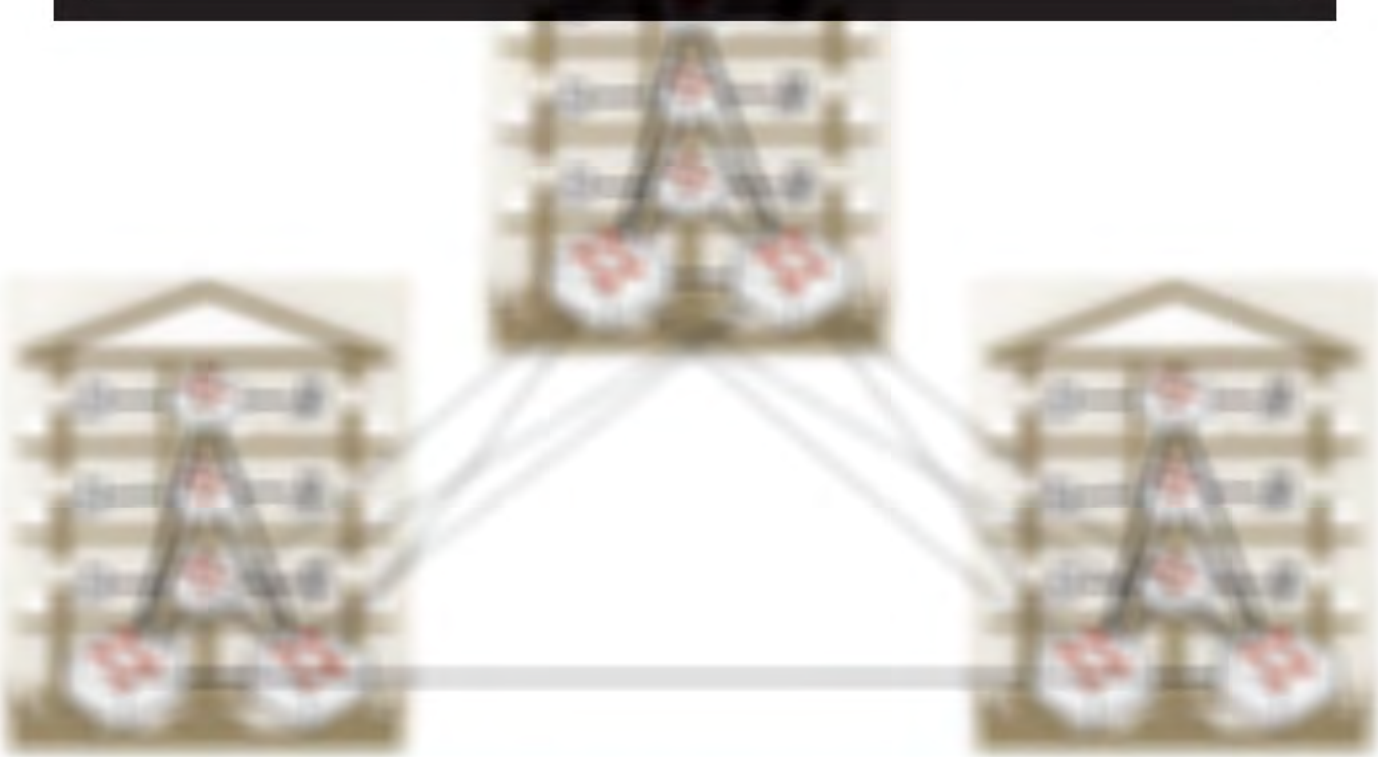
[redacted]

[redacted]



View every page:

http://www.professormesser.com/icnd1



1.7 - Troubleshooting Methodologies

Fault isolation and documentation

- Identify where the problem might be
  - And where it is not
- Limit the scope and save time
  - Random guesses aren't efficient
- Documentation
  - We don't document enough
  - Someone may have done this before
  - Capture your unique local perspective

Resolve or escalate

- The clock is ticking
  - And time is almost always directly relatable to money
- You're looking for the root cause
  - Address the root cause and solve the issue
- What happens if the root cause can't be found?
  - Escalate to the next person/organization in the list
- Your organization may have an escalation process
  - Balances time with money

Verify and monitor

- Does your proposed fix work?
  - Test and confirm
- Some fixes require ongoing monitoring
  - Intermittent issues
  - Confirm the resolution
  - May take minutes, hours, or days
- Don't forget to document
  - It will save you next time

1.8 - IPv4 Addressing

Class	Leading Bits	Network Bits	Remaining Bits	Number of Networks	Hosts per Network	Default Subnet Mask
Class A	0xxx (1-126)	8	24	128	16,777,214	255.0.0.0
Class B	10xx (128-191)	16	16	16,384	65,534	255.255.0.0
Class C	110x (192-223)	24	8	2,097,152	254	255.255.255.0
Class D (multicast)	1110 (224-239)	Not defined	Not defined	Not defined	Not defined	Not defined
Class E (reserved)	1111 (240-254)	Not defined	Not defined	Not defined	Not defined	Not defined

Class A

255	0	0	0
11111111	00000000	00000000	00000000
Network (8)	Hosts (24)		

Class B

255	255	0	0
11111111	11111111	00000000	00000000
Network (16)		Hosts (16)	

Class C

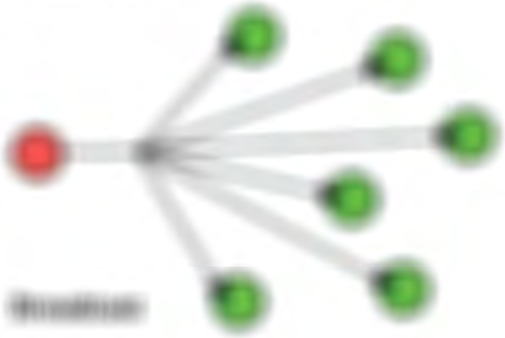
255	255	255	0
11111111	11111111	11111111	00000000
Network (24)			Hosts (8)

The construction of an IPv4 subnet

- Network address
  - The first IP address of a subnet
  - Set all host bits to 0 (0 decimal)
- First usable host address
  - One number higher than the network address
- Network broadcast address
  - The last IP address of a subnet
  - Set all host bits to 1 (255 decimal)
- Last usable host address
  - One number lower than the broadcast address

表 1-1 [illegible]

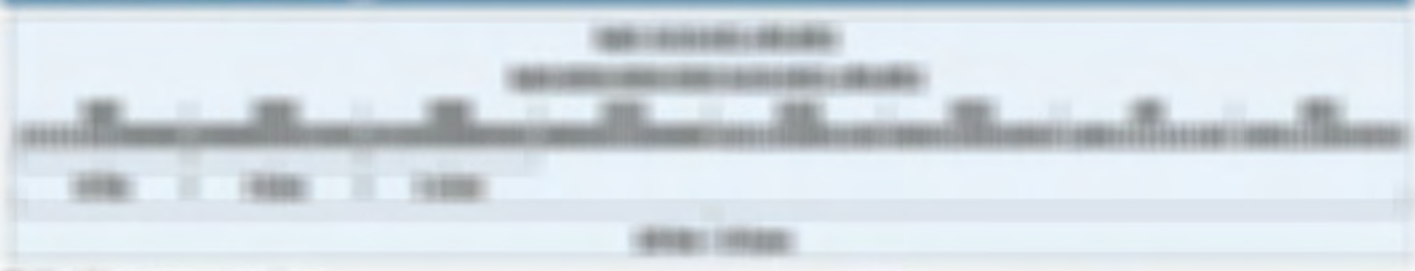
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]



See all of these great notes:

http://www.professormesser.com/icnd1

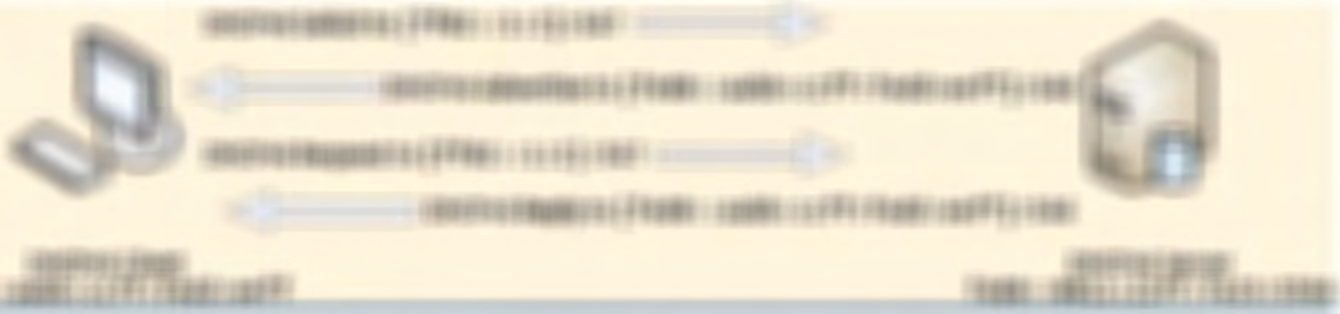
[illegible]



[illegible]

[illegible]

[illegible]



[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

1.14 - IPv6 Address Types (continued)

Link local

- Communicate on the local subnet
  - Every IPv6 interface gets a link local address
- `fe80::/10`
  - `fe80` + 54 zero bits + 64 bit interface ID
  - Effectively becomes `fe80::/64`
- Routers won't forward these packets
  - Everything stays on the local network
- Used mostly for administrative purposes
  - Routing, Neighbor Discovery Protocol, etc.

Solicited-node multicast address

- Every device creates an IPv6 solicited-node multicast address
  - Commonly used in NDP
  - Uses `FF02::1:FF/104`

Solicited-Node	Last 6 Hex

`FF02:0000:0000:0000:0000:0001:FF**:****`

- Local subnet
- Based on the IPv6 unicast address

Multicast

- Communicate to multiple devices simultaneously
  - Without communicating to everyone
- Commonly used for routing protocols
  - Only routers running that protocol will listen
- Multicast addresses start with 1111 1111
  - `FF00::/8`

Prefix	Scope
`ff02::`	Link local - All devices on the local network
`ff05::`	Site local - All devices at a site
`ff08::`	Organization local - All sites within the same organization
`ff0e::`	Global scope - IANA assigned
`ff01::`	Interface local - A multicast loopback

Modified EUI-64

- Use the MAC address to create a static IPv6 address
  - You just need the IPv6 prefix
- Add additional bits to the 48-bit MAC address to create an EUI-64 address
  - Flip the 7th bit and add `FF:FE`
- Easy to configure
  - Takes seconds
  - Always the same IPv6 address
- See more:
  Configuring IPv6 Addresses

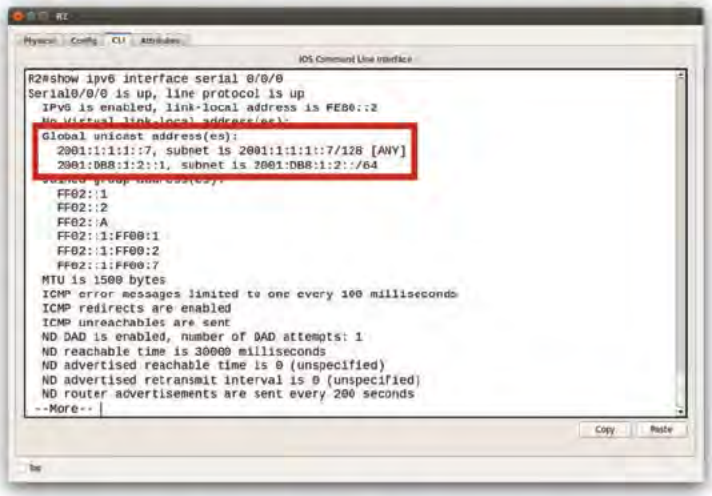
Autoconfiguration

- Stateful autoconfiguration
  - DHCPv6
  - IP address settings are determined by the DHCP server
- Stateless address autoconfiguration (SLAAC)
  - Use NDP to determine the subnet prefix
  - Use the modified EUI-64 to complete the address
  - No server needed
- More:
  IPv6 Addressing with DHCP and SLAAC

Anycast

- Configure the same IPv6 anycast address on different devices
  - Looks like any other unicast address
- Packets sent to an anycast address are delivered to the closest interface
  - Announce the same route out of multiple data centers
  - Clients use the data center closest to them
  - Anycast DNS

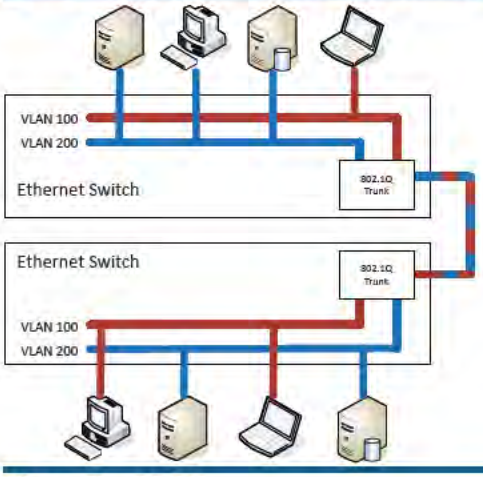
```
# ipv6 address 2001:1:1:1::7/128 anycast
```



[illegible]

[illegible]

2.5 - Configuring Interswitch Connectivity



802.1Q trunking

- Take a normal Ethernet frame

Preamble	SFD	Destination MAC	Source MAC	Type	Payload	FCS

- Add a VLAN header in the frame

Preamble	SFD	Destination MAC	Source MAC	VLAN	Type	Payload	FCS

- VLAN IDs - 12 bits long, 4,094 VLANs
  - "Normal range" - 1 through 1005, "Extended range" - 1006 through 4094
  - 0 and 4,095 are reserved VLAN numbers
- Before 802.1Q, there was ISL (Inter-Switch Link)
  - ISL is no longer used; everyone now uses the 802.1Q standard

The native VLAN

- This is different than the "default VLAN"
  - The default VLAN is the VLAN assigned to an interface by default
- Each trunk has a native VLAN
  - The native VLAN doesn't add an 802.1Q header
- The native VLAN connects switches without a tag
  - Some devices won't talk 802.1Q
  - Just use the native VLAN!
- Native VLAN should match between switches
  - You'll get a message if the VLAN IDs don't match

Trunk configuration

- Use `#switchport mode trunk`
  - Configures a trunk to use all known VLANs
- Dynamic Trunking Protocol (DTP)
  - Automatically configures trunking parameters
- Define the type of trunk
  - IEEE 802.1Q, ISL, or negotiate
- Define the administrative mode
  - Do not trunk, always trunk, or negotiate a trunk

Switchport modes

- `access`
  - A non-trunked port
- `trunk`
  - A trunk port
- `dynamic desirable`
  - Initiates and responds to trunk negotiation messages
- `dynamic auto`
  - Does not initiate, but does respond to trunk negotiation messages

Trunk commands

- `Switch(config-if)#switchport mode access`
- `Switch(config-if)#switchport mode trunk`
- `Switch(config-if)#switchport mode dynamic desirable`
- `Switch(config-if)#switchport mode dynamic auto`

- `Switch#show interfaces trunk`
- `Switch#show vlan id 1`

2.5 - Troubleshooting Interswitch Connectivity

Troubleshooting VLAN configurations

- Check VLAN assignments on the switch
  - This is one of the most common issues you'll find
- Check VLAN assignments between switches
  - This issue usually appears during initial configuration
- Verify the list of trunked VLANs
  - Create good documentation!
- Check the dynamic trunk assignments
  - Another initial config gone wrong

Checking VLAN assignments

- List all VLANs and their associated interfaces

  `Switch#show vlan brief`

  `Switch#show vlan`
- List all interfaces associated with a specific VLAN

  `Switch#show vlan id 1`
- View a specific interface VLAN configuration

  `Switch#show interfaces f0/1 switchport`
- View a list of MAC addresses and their VLAN assignments

  `Switch#show mac address-table`

Dynamic trunking

- Both switches have to be configured with the right trunking mode
  - Don't configure both sides as dynamic auto
  - It's not as "auto" as you might like
- Don't configure dynamic trunking on one side and static on the other
  - You'll end up with an access port with no trunking


Read more about this book:
http://www.professormesser.com/icnd1

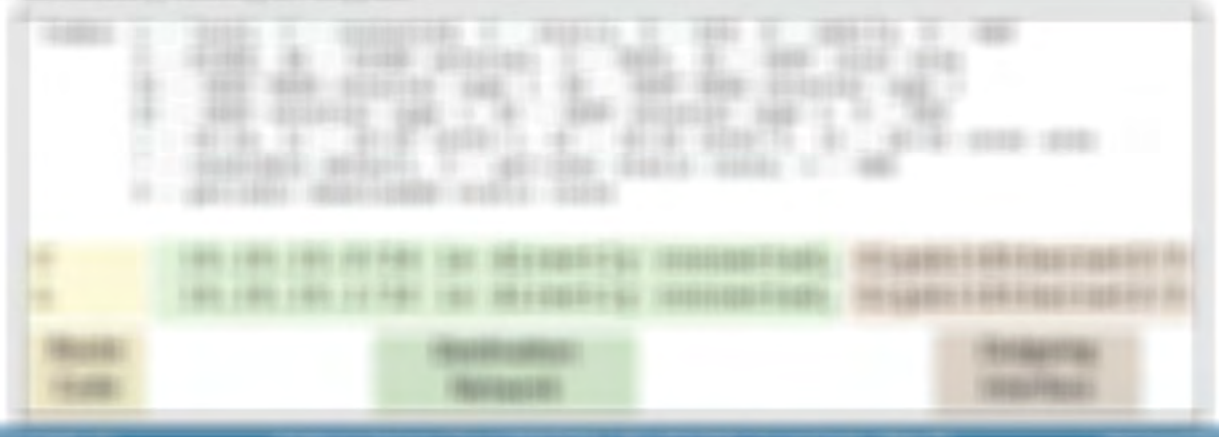
[illegible]

[illegible]

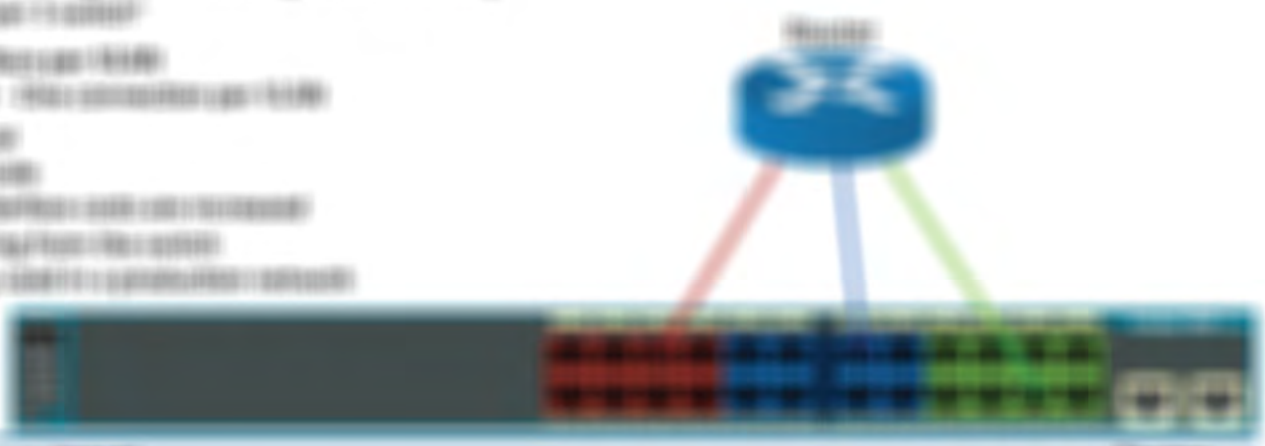
[illegible]

[illegible]

[illegible]



[redacted]



[redacted]

[redacted]

3.6 - IPv4 Static Routing

Host and network routes

- Static route next hop can be an IP address or interface

```
Router1(config)#ip route 10.10.20.0 255.255.255.0 10.10.50.2
Router1(config)#ip route 10.10.20.0 255.255.255.0 s0/3/0
```

- Destination is based on the most specific route
  - A mask of "all ones" is the most specific
- Route to a specific IP address/host
  - Use a mask of 255.255.255.255

```
Router1(config)#ip route 10.10.20.3 255.255.255.255 10.10.50.2
```

```
Router1#show ip route static
     10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
S       10.10.20.0/24 is directly connected, Serial0/3/0
S       10.10.20.2/32 [1/0] via 10.10.40.2
```

Next hop IP address vs. interface

- Static route to next hop IP address
  - Forwarding router needs the L2 address of the next hop IP address
  - ARP for 10.10.50.2, rewrite the L2 frame and send it to the resolved MAC
- Static route to next hop interface
  - Forwarding router assumes the destination IP address is directly connected
  - ARP is sent to the destination IP address through the next hop interface
- Point-to-point connections
  - Use next hop interface or next hop IP address
- Multipoint connections
  - Use next hop IP address

```
Router1(config)#ip route 10.10.20.0 255.255.255.0 10.10.50.2
Router1(config)#ip route 10.10.20.0 255.255.255.0 s0/3/0
```

Populating a static route

- Static route with next hop interface
  - Interface has to be up/up
- Static route with next hop IP address
  - Must have a route to the IP address
- Without these, a route doesn't appear in the table
  - Never shows up
- Force a route to appear with the permanent keyword

```
Router1(config)#ip route 10.10.20.3 255.255.255.255 S0/0/1 permanent
```

- The interface or route still has to be available
  - The packets are dropped otherwise

Default routes

- A route when no other route matches
  - The "gateway of last resort"
- A remote site may have only one route
  - Go that way -> rest of the world
- Can dramatically simplify the routing process
  - Works in conjunction with all other routing methods

```
Router2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.10.40.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.10.20.0/24 is directly connected, GigabitEthernet0/0
L       10.10.20.1/32 is directly connected, GigabitEthernet0/0
C       10.10.40.0/24 is directly connected, Serial0/3/0
L       10.10.40.2/32 is directly connected, Serial0/3/0
S*   0.0.0.0/0 [1/0] via 10.10.40.1
```

There's a lot more right here:

http://www.professormesser.com/icnd1

3.7 - An Overview of RIPv2

Dynamic routing protocols
- Listen for subnet information from other routers
  - Sent from router to router
- Provide subnet information to other routers
  - Tell other routers what you know
- Determine the best path based on the gathered information
  - Every routing protocol has its own way of doing this
- When network changes occur, update the available routes
  - Different convergence process for every dynamic routing protocol

IGP (Interior Gateway Protocol)
- Used within a single autonomous system (AS)
  - Not intended to route between AS
  - That's why there's Exterior Gateway Protocols (EGPs)
- IPv4 dynamic routing
  - OSPFv2 (Open Shortest Path First)
  - RIPv2 (Routing Information Protocol version 2)
  - EIGRP (Enhanced Interior Gateway Routing Protocol)
- IPv6 dynamic routing
  - OSPFv3
  - EIGRP for IPv6
  - RIPng (RIP next generation)

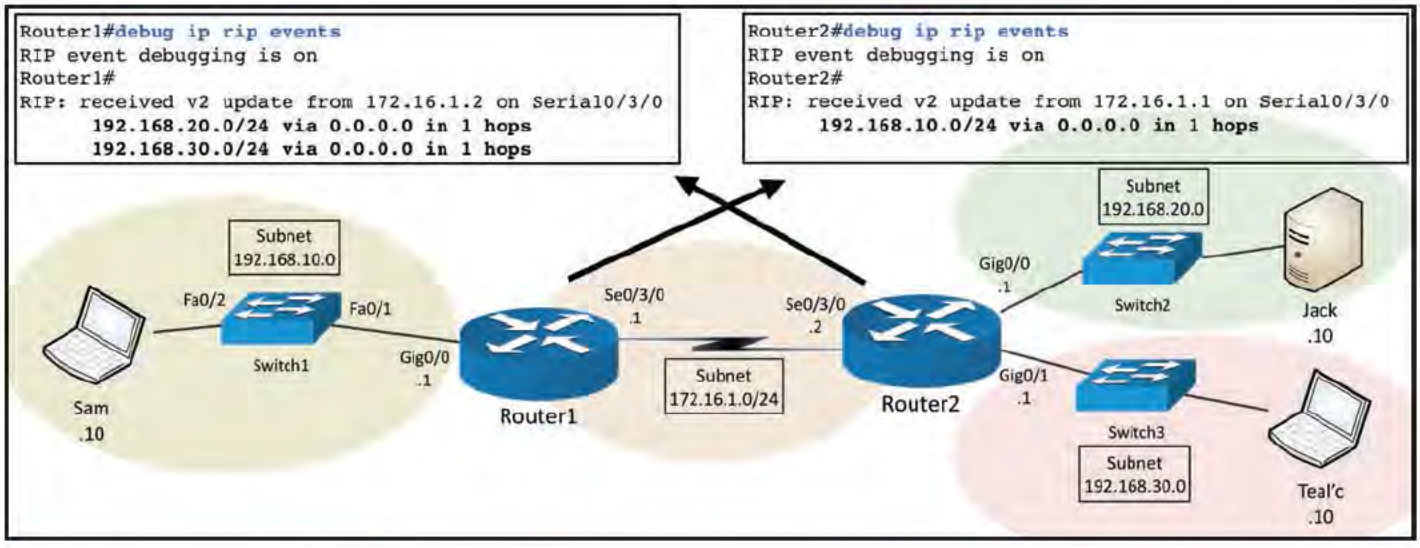
Which routing protocol to use?
- What exactly is a route?
  - Is it based on the state of the link?
  - Is it based on how far away it is?
- How does the protocol determine the best path?
  - Some formula is applied to the criteria to create a metric
  - Rank the routes from best to worst
- Recover after a change to the network
  - Convergence time can vary widely between routing protocols
- Standard or proprietary protocol?
  - OSPF and RIP are standards, basic functions of EIGRP are standard (RFC 7868)

Link state routing protocols
- Information passed between routers is related to the current connectivity
  - If it's up, you can get there.
  - If it's down, you can't.
- Consider the speed of the link
  - Faster is always better, right?
- Very scalable
  - Used most often in large networks
- OSPF, IS-IS
  - Large, scalable routing protocols

Distance-vector routing protocols
- Information passed between routers contains routing tables
  - How many "hops" away is another network?
  - The deciding "vector" is the "distance"
- Usually automatic - very little configuration
- Good for smaller networks
  - Doesn't always scale well to very large networks
- RIP, RIPv2, BGP

```
Router1#debug ip rip events
RIP event debugging is on
Router1#
RIP: received v2 update from 172.16.1.2 on Serial0/3/0
     192.168.20.0/24 via 0.0.0.0 in 1 hops
     192.168.30.0/24 via 0.0.0.0 in 1 hops
```

```
Router2#debug ip rip events
RIP event debugging is on
Router2#
RIP: received v2 update from 172.16.1.1 on Serial0/3/0
     192.168.10.0/24 via 0.0.0.0 in 1 hops
```



[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

4.4 - Troubleshooting DHCP

Confirm your relay agent

- If the DHCP server isn't in your IP subnet, you need an **ip helper-address**
  - If the DHCP server is local, no relay is required
- Router-on-a-stick
  - Separate subnets
  - Need an **ip helper-address** on each subinterface
- Use **show ip interface**
  - Useful when you can't view the configuration

```
Router2#show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 10.10.30.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 172.16.1.1
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
...
```

No DHCP address assigned

- The DHCP relay agent uses the relay interface IP address as the source IP address
  - The DHCP server compares the network configuration to the relay IP address
  - The subnet mask sets the range
- DHCP relay interface and DHCP pool network range must match
  - Without a match, an IP address is not offered
- If you have connectivity, then make the comparison
  - Check the **ip helper-address** interface
  - Compare it to the **network** configuration in the pool

DHCP address is assigned with bad info

- It's easy to mis-configure a DHCP pool
  - So many configuration options
  - You may not have the right address information
- Incorrect default gateway assigned
  - Communicates to devices on the local subnet only
- Incorrect DNS values
  - No name resolution, but IP works
- TFTP address is incorrectly assigned
  - VoIP phone doesn't download a configuration file

It's ~~never~~ always the network

- Centralized DHCP servers rely on a stable/valid network connection
  - You can't get an IP address unless there's a link
- Use **ping** and **traceroute** to validate the connection
  - The link between the DHCP relay interface and the ip helper-address

Between the DHCP client and the relay

- DHCP is all about broadcasts
  - 255.255.255.255 - "all ones" broadcast
- Routers do not forward DHCP broadcast packets
  - Or any other broadcast packets
- Make sure the DHCP client is a VLAN with an **ip helper-address**
  - Broadcasts are very limiting
  - Basic connectivity is required

DHCP troubleshooting

- Confirm the **ip helper-address** interfaces and IP addresses
  - One wrong interface or address is fatal
- DHCP pool **network** configuration should match relay interface IP
  - Check a pool's IP addresses and subnet masks
- Check the network between DHCP server IP address and DHCP relay IP address
  - Connectivity is critical
- Check local LAN between the DHCP relay agent and the DHCP client
  - Easy to be placed in the wrong VLAN

4.5 - Configuring NTP

NTP (Network Time Protocol)

- Switches, routers, firewalls, servers, workstations - Every device has its own clock
- Synchronizing the clocks becomes critical - Log files, authentication information, outage details
- Automatic updates - no flashing 12:00 lights
- Flexible - you control how clocks are updated
- Very accurate - Accuracy is better than 1 millisecond on a local network

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

4.6 - Configuring Standard Numbered Access Lists

Standard numbered ACLs

- Standard ACL
  - Source IP address is the only criteria
- Numbered ACL
  - ACLs are referenced by number instead of a name

ACL syntax

- Standard numbered ACLs use access list numbers between 1-99 or 1300-1999
  - The gap is reserved for other protocols (AppleTalk, DECnet, IPX, etc.)

```
router(config)#access-list {1-99 | 1300-1999}
    {permit | deny} {source [source-wildcard] | any}
router(config)#access-list 1 deny 10.10.1.77
router(config)#access-list 1 permit all
```

Configuring standard numbered ACLs

- Choose router interface and direction
  - Put a standard ACL near the destination IP - prevents inadvertent discards
  - Use the Source IP address - make sure to use the correct direction
- Create the ACLs using global configuration commands
  - Top-down matching - default is to deny if nothing else matches
- Add the ACL to the interface

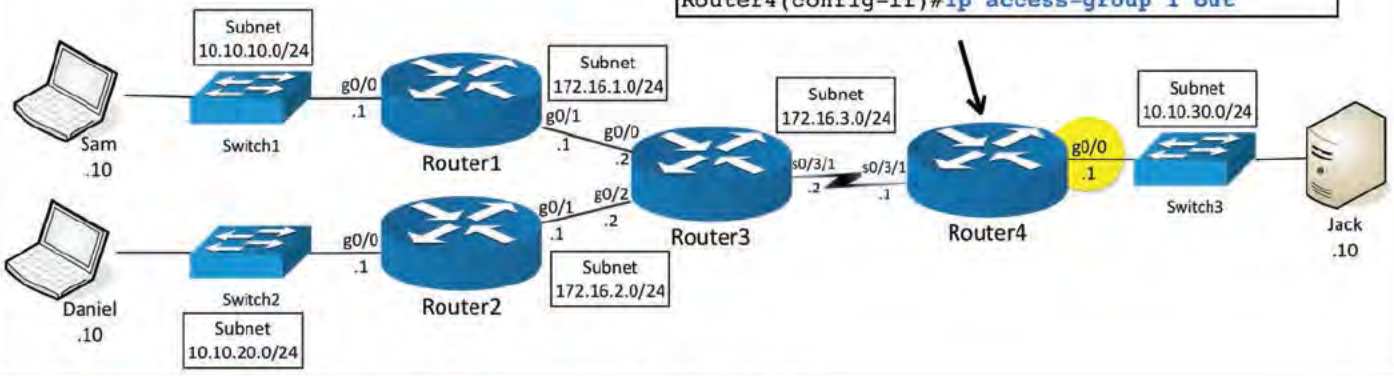
```
ip access-group 1 in
ip access-group 2 out
```

Viewing ALC configuration information

- `Rtr4#show ip access-lists`
  - View all ACLs
- `Rtr4#show ip interface g0/0`
  - Interface information shows which ingoing and outgoing ACLs are associated with the interface

- Prevent Sam from accessing Jack's server
- Pick a location closest to the destination

```
Router4(config)#access-list 1 deny 10.10.10.10
Router4(config)#access-list 1 permit any
Router4(config)#int g0/0
Router4(config-if)#ip access-group 1 out
```

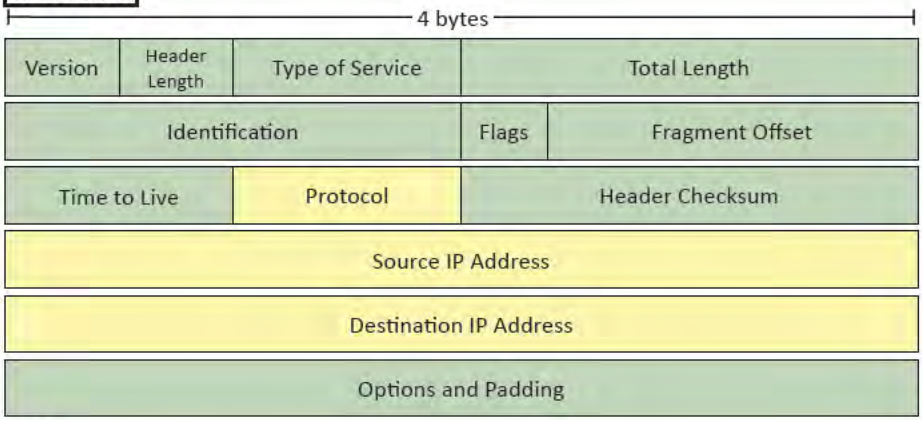


4.6 - Configuring Extended Numbered Access Lists

Extended numbered access lists

- Similar to standard numbered ACLs
  - Top-down first-match logic, ingress or egress filtering
- Now you'll have many more filtering options
  - Source IP address, destination IP address, protocol

IP Header



Extended numbered IPv4 ACL

- Syntax is similar to the standard number ACLs
  - Adds additional matching keywords
- Uses number ranges 100-199 and 2000-2699
- protocol - ip, tcp, udp, icmp

```
access list 101 deny icmp any any
```

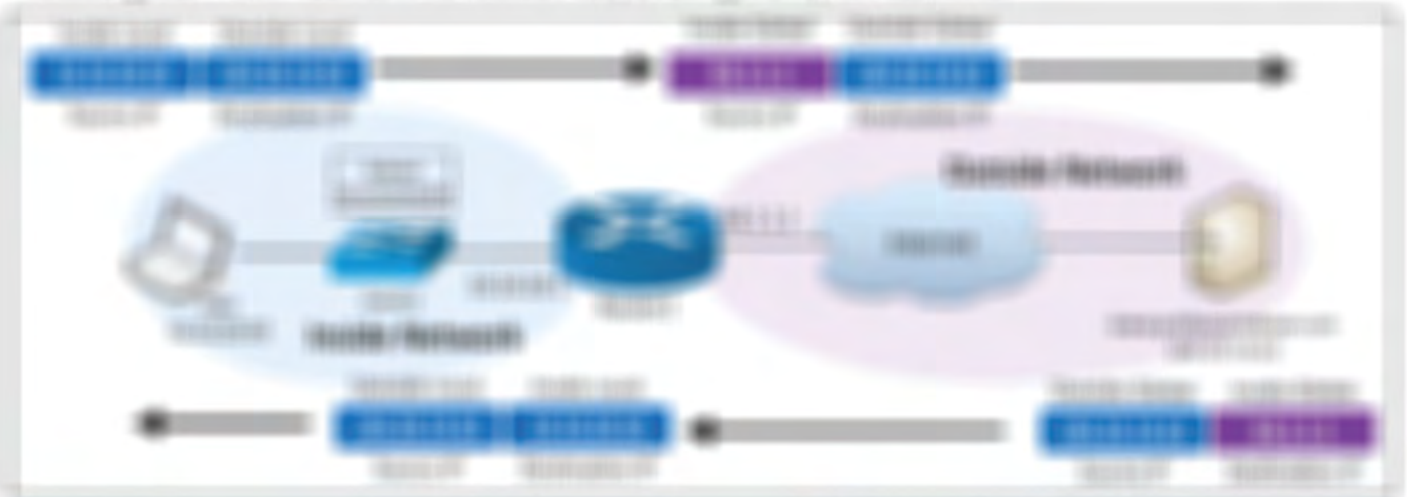
- source_ip, source_port, dest_ip, dest_port

```
access list 101 deny tcp 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255 eq 80
```

[illegible]

[illegible]

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]


Internet / Network

[illegible]

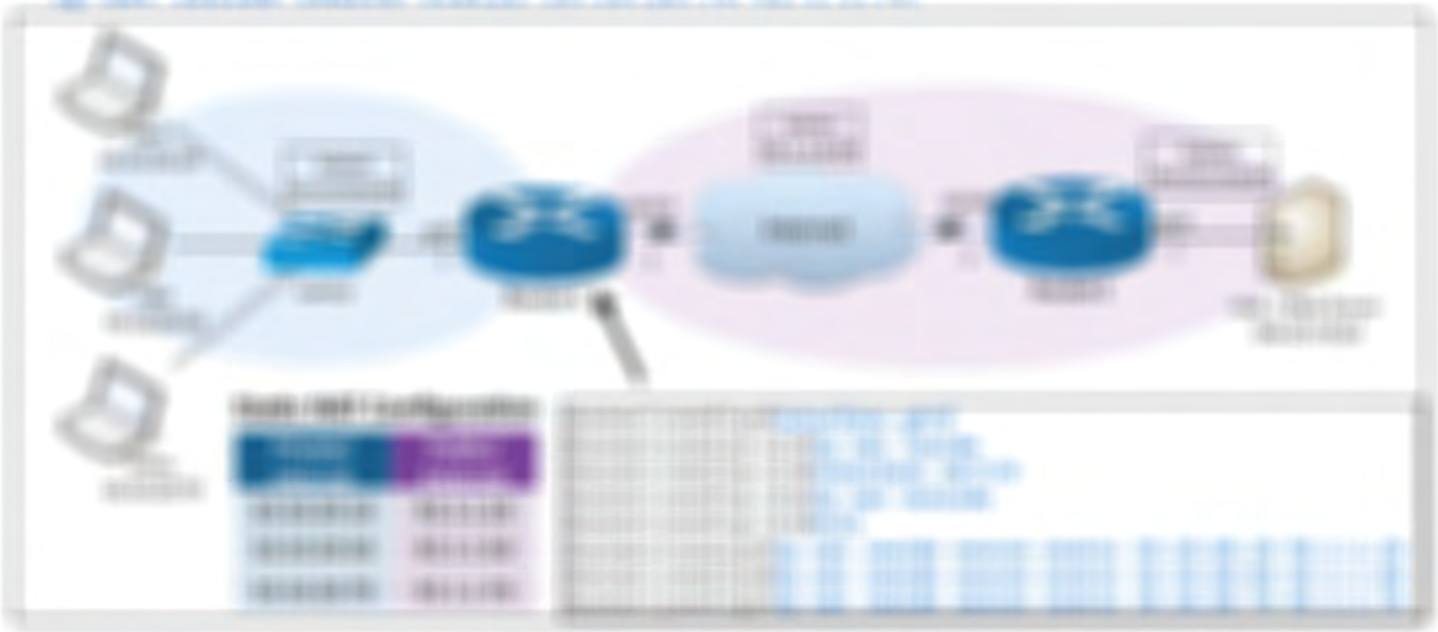
[illegible]

[illegible]

[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]



[redacted]

```
[redacted]
```

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

```
[redacted]
```

4.7 - Configuring Network Address Translation (continued)

Monitoring NAT overload/PAT

```
Router1#show ip nat statistics
Total translations: 3 (0 static, 3 dynamic, 3 extended)
Outside Interfaces: Serial0/3/0
Inside Interfaces: GigabitEthernet0/0
Hits: 68  Misses: 35
Expired translations: 0
Dynamic mappings:
```

```
Router1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 92.1.1.1:1024      10.10.20.50:1027   104.20.19.63:80    104.20.19.63:80
tcp 92.1.1.1:1025      10.10.20.70:1027   104.20.19.63:80    104.20.19.63:80
tcp 92.1.1.1:1027      10.10.20.10:1027   104.20.19.63:80    104.20.19.63:80
```

4.7 - Troubleshooting Network Address Translation

Troubleshooting best-practices

- Check your directions
  - **`ip nat inside`** and **`ip nat outside`** are easy to swap
- The inside interface triggers the translation

Other troubleshooting challenges

- Unintended ACLs
  - We need ACL for dynamic NAT/PAT to work
  - Other configured ACLs might drop traffic before we can NAT
  - ACLs are processed before the NAT occurs
- NAT needs traffic to work
  - The show ip nat translation table will be empty without user traffic
- The network must function correctly
  - All routes need to work properly

Static NAT troubleshooting

- Order is important
  - Inside local address is first, inside global address is second

```
Router1(config)#interface g0/0
Router1(config-if)#ip nat inside
Router1(config-if)#interface s0/3/0
Router1(config-if)#ip nat outside
Router1(config-if)#exit
Router1(config)#ip nat inside source static 10.10.20.10 92.1.1.10
Router1(config)#ip nat inside source static 10.10.20.50 92.1.1.50
Router1(config)#ip nat inside source static 10.10.20.70 92.1.1.70
```

Dynamic NAT ACL

- The ACL has to match, so double check your logic
- All ACL IP address matches are pre-NAT addresses

```
Router1(config)#interface g0/0
Router1(config-if)#ip nat inside
Router1(config-if)#interface s0/3/0
Router1(config-if)#ip nat outside
Router1(config-if)#exit
Router1(config)#access-list 1 permit 10.10.20.0 0.0.0.255
Router1(config)#ip nat pool midway 94.1.1.1 94.1.1.2 netmask 255.255.255.0
Router1(config)#ip nat inside source list 1 pool midway
```

Dynamic NAT pool

- Make sure you have enough addresses
- The NAT will work for some but not for others
- Check the number of misses in **`show ip nat statistics`**
- You'll see when the NAT isn't working

```
Router1(config)#interface g0/0
Router1(config-if)#ip nat inside
Router1(config-if)#interface s0/3/0
Router1(config-if)#ip nat outside
Router1(config-if)#exit
Router1(config)#access-list 1 permit 10.10.20.0 0.0.0.255
Router1(config)#ip nat pool midway 94.1.1.1 94.1.1.2 netmask 255.255.255.0
Router1(config)#ip nat inside source list 1 pool midway
```

NAT overload / PAT troubleshooting

- Almost identical to dynamic NAT
- The only significant difference is the overload keyword
- Don't forget the overload parameter
- You'll run out of addresses very quickly

```
Router1(config)#interface g0/0
Router1(config-if)#ip nat inside
Router1(config-if)#interface s0/3/0
Router1(config-if)#ip nat outside
Router1(config-if)#exit
Router1(config)#access-list 1 permit 10.10.20.0 0.0.0.255
Router1(config)#ip nat inside source list 1 interface s0/3/0 overload
```

[illegible]

[illegible]

5.3 - Initial Device Configuration

Booting IOS

- Performs a POST
  - Power On Self Test
  - Basic hardware check
- Boots from ROM
  - Bootstrap program is copied into RAM
- Bootstrap boots an IOS image or ROM Monitor (ROMMON)
  - ROMMON is used for administrative and maintenance purposes
- IOS loads the startup-config file
  - Loaded into RAM as `running-config`

Initial device configuration

- No configuration file? No problem.
- System Configuration Dialog (Setup Mode)
  - Menu-driven configuration on a new device
- You don't have to use Setup Mode
  - Configure the dvevice through **`configure terminal`**

What you'll need

- Hostname
- Enable secret password
  - Protects privileged EXEC and configuration modes
- Enable password
  - A less-secure version of the enable secret password
  - Remove it after configuring the device
- Virtual terminal password
  - The password used when accessing the device over the network
- Configure SNMP management (yes or no)
- Physical interface for management
  - Need IP address and subnet mask

5.4 - Configuring IOS Passwords

Authenticating to IOS devices

- Most organizations will use an external AAA server
  - Authentication, Authorization, and Accounting
  - No passwords on the IOS device
- You might want a backup login
  - Just in case
- Potential security concern
  - Store the passwords securely

Teletype lines

- Inbound connections are made over TTY lines
  - Many different TTY lines on an IOS device
- CTY - Console interface
- TTY - Asyncronous serial interfaces
- AUX - Auxiliary port
- VTY - Virtual teletype/virtual terminal
- View with **`show line`**

User mode and privileged mode passwords

- Console password
  - Protects connections through the console port
- vty password
  - Protects connections through the virtual teletype port (telnet or SSH)
- Enable password
  - Prompts when entering enable mode
- With no passwords configured, no passwords are required
  - A bad idea

Authenticating to IOS devices

- Most organizations will use an external AAA server
  - Authentication, Authorization, and Accounting
  - No passwords on the IOS device
- You might want a backup login
  - Just in case
- Potential security concern
  - Store the passwords securely

Configuring lines

- Console password

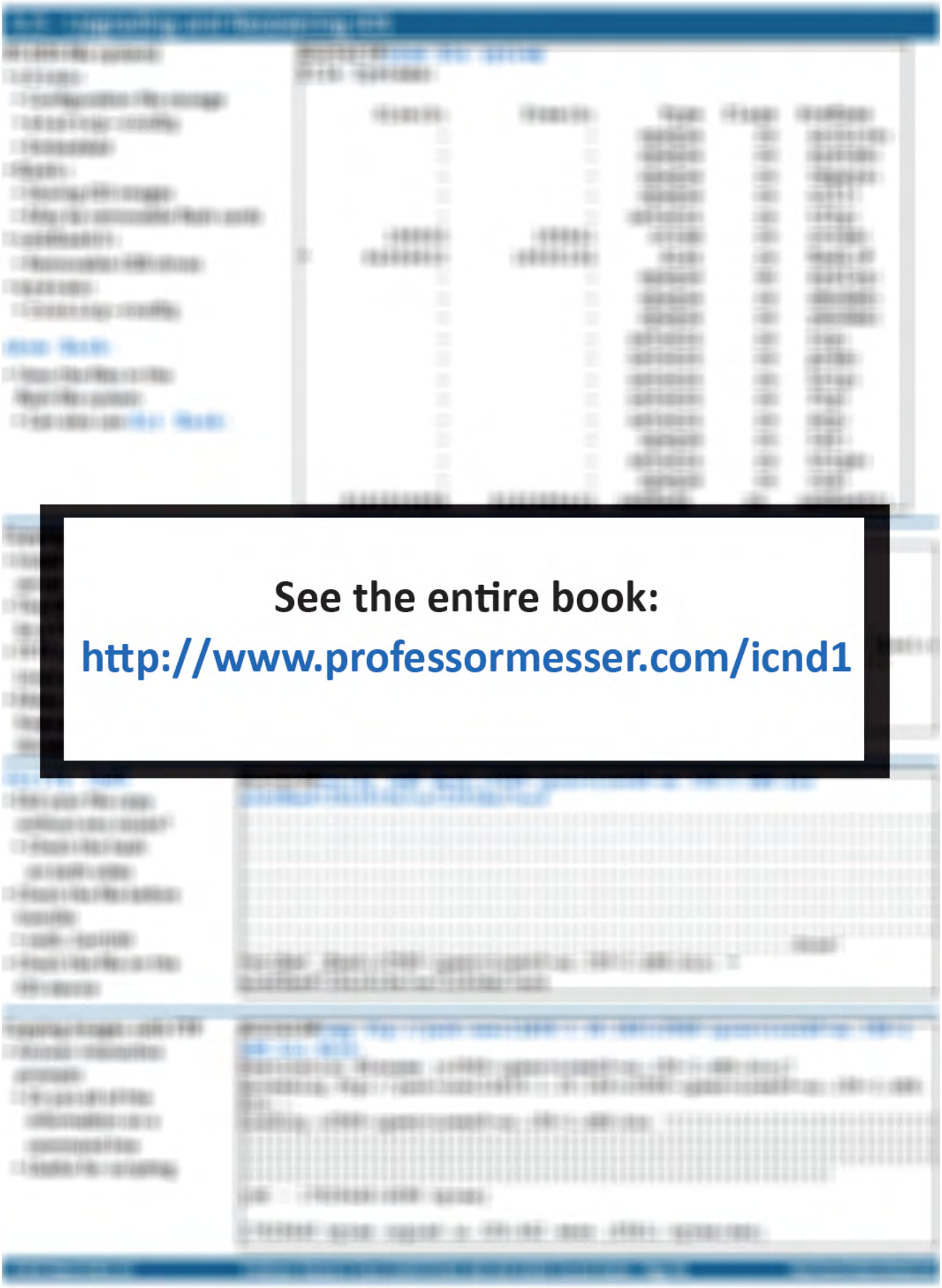
```
Router1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#line console 0
Router1(config-line)#password sgc
Router1(config-line)#login
```

- Telnet/SSH password

```
Router1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#line vty 0 4
Router1(config-line)#password sg1
Router1(config-line)#login
```

- Enable/Privileged EXEC mode password

```
Router1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#enable secret cheyenne
```



See the entire book:

http://www.professormesser.com/icnd1

[illegible]

[illegible]

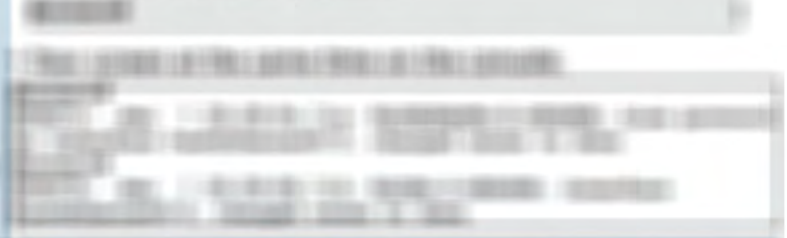
[illegible]

[illegible]

[illegible]

[illegible]

[illegible]



5.6 - Logging at the Terminal (continued)

terminal monitor

- Monitor the logs in an SSH session

```
Router4#terminal monitor
Router4#
000078: Mar  7 20:58:18.303: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to down
000079: .Mar  7 20:58:19.327: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
Router4#
000080: .Mar  7 20:58:20.342: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to down
Router4#
000081: .Mar  7 20:58:28.562: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to up
000082: .Mar  7 20:58:29.569: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
Router4#
000083: .Mar  7 20:58:56.656: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up
Router4#
```

```
Router4#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
                         0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

    Console logging: level debugging, 83 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 6 messages logged, xml disabled,
                     filtering disabled
        Logging to: vty1(6)
    Buffer logging:  level debugging, 83 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    File logging: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level informational, 87 message lines logged
        Logging Source-Interface:       VRF Name:

Log Buffer (4096 bytes):
8.137: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to up
```

Severity levels

- Logging levels can be individually configured
  - Each service can have it's own verbosity
  - Logs are displayed for that level and lower (more severe)
- Console logs
  logging console 7
- Monitor logs
  logging monitor 6
- Internal buffer logs
  logging buffered 4
- Syslog
  logging trap 6

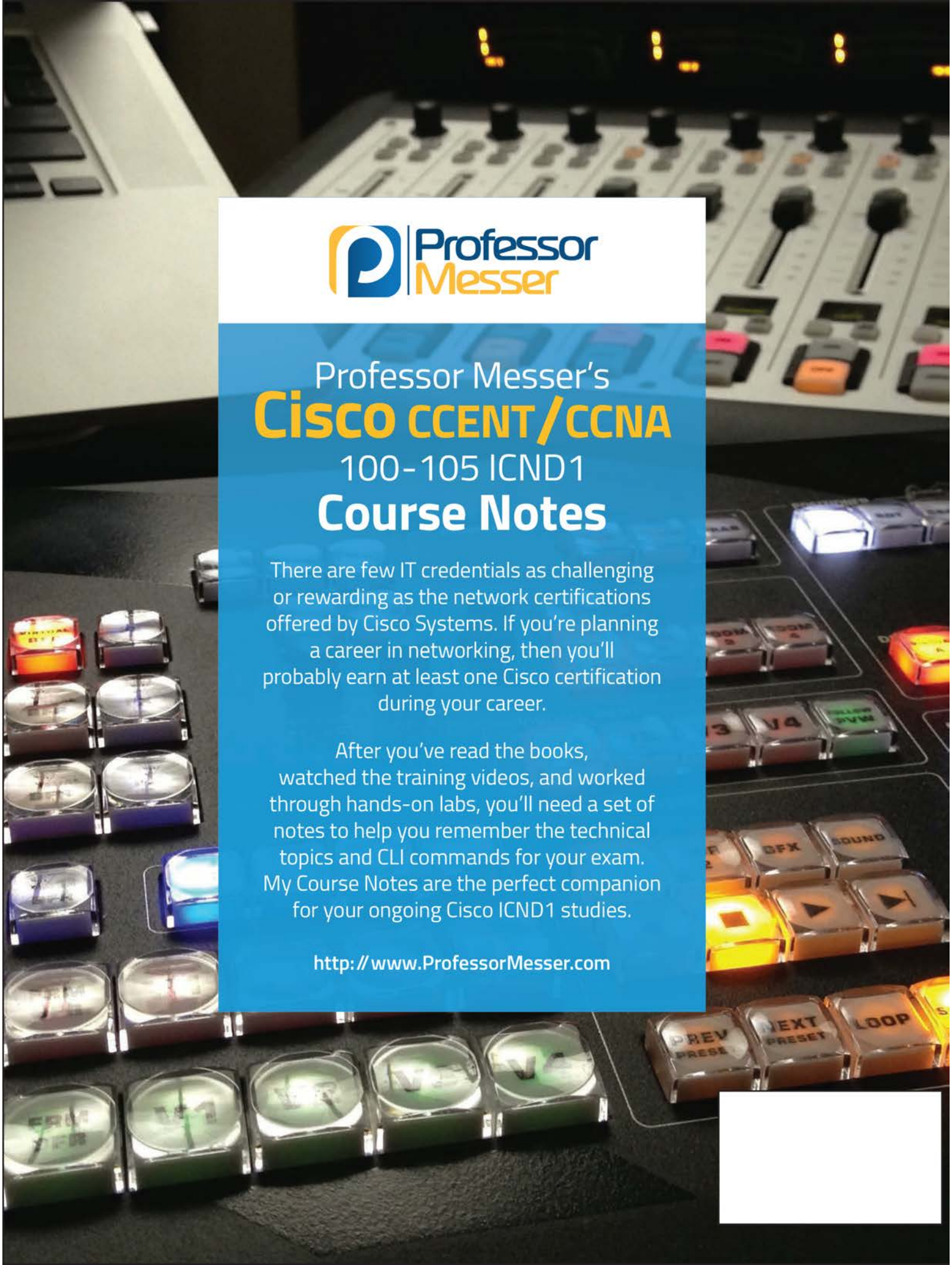
Severity Level	Keyword	Description
0	emergencies	System unstable
1	alerts	Immediate action needed
2	critical	Critical conditions
3	errors	Error conditions
4	warnings	Warning conditions
5	notifications	Normal but significant condition
6	informational	Informational messages only
7	debugging	Debugging messages

Debugging

- Monitor IOS internal processes
  - Many different debug options
- Enabling debug will use additional resources
  - Make sure you have the overhead
  Router4#show process cpu
- If you're connecting over ssh, be sure to enable logging
  Router4#terminal monitor

Thank you for viewing this sample of my ICND1 Course Notes. Good studies!

http://www.professormesser.com/icnd1


Professor Messer
Professor Messer's
Cisco CCENT/CCNA
100-105 ICND1
Course Notes
There are few IT credentials as challenging or rewarding as the network certifications offered by Cisco Systems. If you're planning a career in networking, then you'll probably earn at least one Cisco certification during your career.
After you've read the books, watched the training videos, and worked through hands-on labs, you'll need a set of notes to help you remember the technical topics and CLI commands for your exam. My Course Notes are the perfect companion for your ongoing Cisco ICND1 studies.
http://www.ProfessorMesser.com