



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



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

Written by James "Professor" Messer

Copyright © 2017 by Messer Studios, LLC

<http://www.ProfessorMesser.com>

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher.

First Edition: March 2017

Trademark Acknowledgements

All product names and trademarks are the property of their respective owners, and are in no way associated or affiliated with Messer Studios, LLC.

"Professor Messer" is a registered trademark of Messer Studios LLC.

"Cisco" and "IOS" are registered trademarks of Cisco Systems, Inc.

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	iv
0.0 - Overview	1
The 100-105 Cisco ICND1 Exam	1
Introduction to the Cisco CLI	1
1.0 - Network Fundamentals	1
1.1 - Introduction to Ethernet - The Ethernet Frame	1
1.1 - The OSI Model and TCP/IP Model	2
1.1 - Encapsulation and decapsulation	3
1.2 - Common Port Numbers	3
1.2 - TCP Header	3
1.2 - UDP Header	4
1.2 - TCP Communication	4
1.3 - Enterprise Infrastructure Components	4
1.4 - Network Architectures	5
1.5 - Network Topologies	6
1.6 - Network Cabling	6
1.7 - Troubleshooting Methodologies	8
1.8 - IPv4 Addressing	8
1.9 - IPv4 Address Types	9
1.10 - Private IPv4 Addressing	10
1.11 - IPv6 Addressing	11
1.12 - Configuring IPv6 Addressing	11
1.12 - Troubleshooting IPv6 Addressing	12
1.13 - IPv6 Neighbor Discovery Protocol	13
1.13 - IPv6 Addressing with DHCP and SLAAC	14
1.14 - IPv6 Address Types	14
2.0 - LAN Switching Fundamentals	16
2.1 - LAN Switching Concepts	16
2.3 - Troubleshooting Cable and Interface Issues	16
2.4 - Introduction to VLANs	18
2.4 - Configuring VLANs	19
2.4 - Troubleshooting VLANs	19
2.5 - Configuring Interswitch Connectivity	20
2.5 - Troubleshooting Interswitch Connectivity	20
2.6 - Configuring CDP and LLDP	21
2.7 - Configuring Port Security	21
2.7 - Troubleshooting Port Security	22
3.0 - Routing Fundamentals	24
3.1 - Introduction to Routing	24
3.2 - Understanding Routing Tables	25
3.3 - Routing Metrics and Administrative Distances	26
3.4 - Router on a Stick and Layer 3 Switches	27
3.5 - Static and Dynamic Routing	28
3.6 - IPv4 Static Routing	29

3.6 - IPv6 Static Routing.....	30
3.6 - Troubleshooting Static Routing.....	31
3.7 - An Overview of RIPv2.....	32
3.7 - Configuring RIPv2.....	33
3.7 - Optional RIPv2 Features.....	34
3.7 - Troubleshooting RIPv2.....	35
4.0 - Infrastructure Services.....	36
4.1 - An Overview of DNS.....	36
4.2 - Troubleshooting DNS.....	36
4.3 - An Overview of DHCP.....	37
4.3 - Configuring DHCP.....	37
4.4 - Troubleshooting DHCP.....	39
4.5 - Configuring NTP.....	39
4.6 - An Overview of Access Lists.....	41
4.6 - Configuring Standard Numbered Access Lists.....	42
4.6 - Configuring Extended Numbered Access Lists.....	42
4.6 - Configuring Named Access Lists.....	43
4.6 - Troubleshooting Access Lists.....	44
4.7 - An Overview of Network Address Translation.....	46
4.7 - Configuring Network Address Translation.....	47
4.7 - Troubleshooting Network Address Translation.....	49
5.0 - Infrastructure Maintenance.....	50
5.1 - Configuring Syslog.....	50
5.2 - Configuration Management.....	51
5.2 - Discovering Devices with CDP and LLDP.....	51
5.2 - Switch and Router Licensing.....	52
5.2 - Configuring Timezones.....	53
5.2 - Configuring Loopback Interfaces.....	53
5.3 - Initial Device Configuration.....	54
5.4 - Configuring IOS Passwords.....	54
5.4 - Configuring Banners.....	55
5.4 - Device Hardening.....	55
5.5 - Upgrading and Recovering IOS.....	56
5.5 - IOS Password Recovery.....	58
5.5 - IOS File System Management.....	59
5.6 - Troubleshooting with Ping.....	60
5.6 - Troubleshooting with Traceroute.....	60
5.6 - Logging at the Terminal.....	60

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 Associate 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 - Infrastructure 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.



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

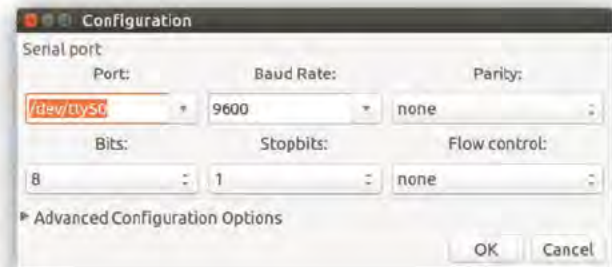
- From the computer
 - 9-pin serial connector or USB interface
- From the switch or router
 - 9-pin serial connector, RJ45 connector, USB interface
- You might need a USB to serial cable
 - And a set of adapters

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

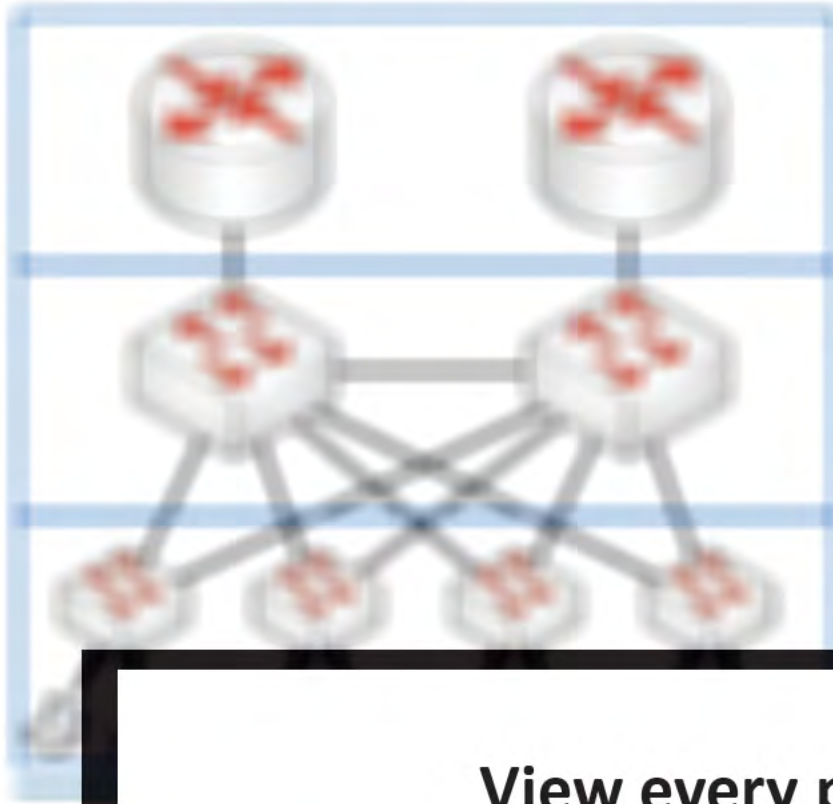
- This must match the settings on the other device
 - A mismatch results in a screen of scrambled text
- Port - The physical interface
- Baud rate - The speed of the data (9600 baud)
- Parity - None
- Data bits - 8
- Stop bits - 1
- Flow control - none



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
----------	-----	-----------------	------------	------	---------	-----



- Hosts (Servers)**
- 1. High speed network access
 - 2. High speed network connections
 - 3. High speed network connections
- Routers**
- 1. High speed network access
 - 2. High speed network connections
 - 3. High speed network connections
- Servers**
- 1. High speed network access

View every page:
<http://www.professormesser.com/icnd1>



1.1.1. **Networks in a star topology**



- Advantages**
- 1. Easy to install and maintain
 - 2. If one node fails, it does not affect the rest of the network
 - 3. Easy to add or remove nodes

- Disadvantages**
- 1. Requires a central device (switch or hub)
 - 2. If the central device fails, the entire network is affected



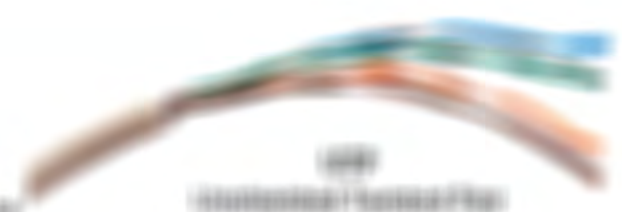
- Advantages**
- 1. High reliability and redundancy
 - 2. Easy to add or remove nodes



1.1.2. **Networks in a ring topology**

- Advantages**
- 1. Easy to install and maintain
 - 2. If one node fails, it does not affect the rest of the network
 - 3. Easy to add or remove nodes

- Disadvantages**
- 1. If one node fails, the entire network is affected
 - 2. If one node fails, the entire network is affected
 - 3. If one node fails, the entire network is affected



- Advantages**
- 1. Easy to install and maintain
 - 2. If one node fails, it does not affect the rest of the network
- Disadvantages**
- 1. If one node fails, the entire network is affected
 - 2. If one node fails, the entire network is affected

- Advantages**
- 1. Easy to install and maintain
 - 2. If one node fails, it does not affect the rest of the network
- Disadvantages**
- 1. If one node fails, the entire network is affected
 - 2. If one node fails, the entire network is affected

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

ICND1 - The Network Layer (continued)

- IPv4 address - binary alternative is available - octets
- IPv4 addresses - network & host portions
- IPv4 address - 32 bits
- IPv4 - not a valid address - 192.168.0.0
- IPv4 - 0.0.0.0

- IPv6 address - binary alternative is available - octets
- IPv6 address - network & host portions
- IPv6 address - 128 bits
- IPv6 address - 128 bits
- IPv6 address - 128 bits
- IPv6 address - 128 bits
- IPv6 address - 128 bits
- IPv6 address - 128 bits

- IPv4 address - binary alternative is available - octets
- IPv4 address
- IPv4 address - network & host portions
- IPv4 address
- IPv4 address - network & host portions
- IPv4 address



See all of these great notes:
<http://www.professormesser.com/icnd1>

- IPv4 address - binary alternative is available - octets
- IPv4 address - network & host portions
- IPv4 address - 32 bits
- IPv4 address - 32 bits
- IPv4 address - 32 bits
- IPv4 address - 32 bits
- IPv4 address - 32 bits
- IPv4 address - 32 bits

IP address range	Number of addresses	Private description	Unicast address (network - host)	Host ID range
10.0.0.0 - 10.255.255.255	16,777,216	single class C	10.0.0.0 - 10.255.255.255	10.0.0.1 - 10.255.255.254
172.16.0.0 - 172.31.255.255	1,048,576	16 contiguous class C	172.16.0.0 - 172.31.255.255	172.16.0.1 - 172.31.255.254
192.168.0.0 - 192.168.255.255	16,777,216	16 contiguous class C	192.168.0.0 - 192.168.255.255	192.168.0.1 - 192.168.255.254

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
<code>ff02::</code>	Link local - All devices on the local network
<code>ff05::</code>	Site local - All devices at a site
<code>ff08::</code>	Organization local - All sites within the same organization
<code>ff0e::</code>	Global scope - IANA assigned
<code>ff01::</code>	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`

```
R2#show ipv6 interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::2
No Virtual link-local address(es):
Global unicast address(es):
2001:1:1:1::7, subnet is 2001:1:1:1::7/128 [ANY]
2001:DB8:1:2::1, subnet is 2001:DB8:1:2::/64
Forwarding group: unicast (0/7)
FF02::1
FF02::2
FF02::A
FF02:1:FF00:1
FF02:1:FF00:2
FF02:1:FF00:7
MTU is 1500 bytes
TCP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
--More--
```


Gegeben: $a_1 = 1$, $a_2 = 1$, $a_3 = 1$, $a_4 = 1$, $a_5 = 1$, $a_6 = 1$, $a_7 = 1$, $a_8 = 1$, $a_9 = 1$, $a_{10} = 1$

Zu zeigen: $a_n = 1$ für alle $n \in \mathbb{N}$

Lösung: $a_1 = 1$, $a_2 = 1$, $a_3 = 1$, $a_4 = 1$, $a_5 = 1$, $a_6 = 1$, $a_7 = 1$, $a_8 = 1$, $a_9 = 1$, $a_{10} = 1$

Induktionsanfang: $a_1 = 1$, $a_2 = 1$, $a_3 = 1$, $a_4 = 1$, $a_5 = 1$, $a_6 = 1$, $a_7 = 1$, $a_8 = 1$, $a_9 = 1$, $a_{10} = 1$

Induktionsschritt: $a_n = 1$ für alle $n \in \mathbb{N}$

Induktionsannahme: $a_k = 1$ für alle $k < n$

Induktionsschluss: $a_n = 1$ für alle $n \in \mathbb{N}$

Induktionsanfang	Induktionsschritt	Induktionsannahme	Induktionsschluss
$a_1 = 1$	$a_2 = 1$	$a_k = 1$	$a_n = 1$
$a_2 = 1$	$a_3 = 1$	$a_k = 1$	$a_n = 1$
$a_3 = 1$	$a_4 = 1$	$a_k = 1$	$a_n = 1$
$a_4 = 1$	$a_5 = 1$	$a_k = 1$	$a_n = 1$
$a_5 = 1$	$a_6 = 1$	$a_k = 1$	$a_n = 1$
$a_6 = 1$	$a_7 = 1$	$a_k = 1$	$a_n = 1$
$a_7 = 1$	$a_8 = 1$	$a_k = 1$	$a_n = 1$
$a_8 = 1$	$a_9 = 1$	$a_k = 1$	$a_n = 1$
$a_9 = 1$	$a_{10} = 1$	$a_k = 1$	$a_n = 1$

Induktionsanfang	Induktionsschritt	Induktionsannahme	Induktionsschluss
$a_1 = 1$	$a_2 = 1$	$a_k = 1$	$a_n = 1$
$a_2 = 1$	$a_3 = 1$	$a_k = 1$	$a_n = 1$

Induktionsanfang	Induktionsschritt	Induktionsannahme	Induktionsschluss
$a_1 = 1$	$a_2 = 1$	$a_k = 1$	$a_n = 1$
$a_2 = 1$	$a_3 = 1$	$a_k = 1$	$a_n = 1$
$a_3 = 1$	$a_4 = 1$	$a_k = 1$	$a_n = 1$
$a_4 = 1$	$a_5 = 1$	$a_k = 1$	$a_n = 1$
$a_5 = 1$	$a_6 = 1$	$a_k = 1$	$a_n = 1$
$a_6 = 1$	$a_7 = 1$	$a_k = 1$	$a_n = 1$
$a_7 = 1$	$a_8 = 1$	$a_k = 1$	$a_n = 1$
$a_8 = 1$	$a_9 = 1$	$a_k = 1$	$a_n = 1$
$a_9 = 1$	$a_{10} = 1$	$a_k = 1$	$a_n = 1$

Zu zeigen: $a_n = 1$ für alle $n \in \mathbb{N}$

Lösung: $a_1 = 1$, $a_2 = 1$, $a_3 = 1$, $a_4 = 1$, $a_5 = 1$, $a_6 = 1$, $a_7 = 1$, $a_8 = 1$, $a_9 = 1$, $a_{10} = 1$

Induktionsanfang: $a_1 = 1$, $a_2 = 1$, $a_3 = 1$, $a_4 = 1$, $a_5 = 1$, $a_6 = 1$, $a_7 = 1$, $a_8 = 1$, $a_9 = 1$, $a_{10} = 1$

Induktionsschritt: $a_n = 1$ für alle $n \in \mathbb{N}$

Induktionsannahme: $a_k = 1$ für alle $k < n$

Induktionsschluss: $a_n = 1$ für alle $n \in \mathbb{N}$

Accounting

Accounting cycle

Accounting cycle

Accounting cycle	Description
1. Analyze the business transactions and events.	Identify the business transactions and events that have an effect on the accounting equation.
2. Journalize the business transactions and events.	Record the business transactions and events in the journal in chronological order.
3. Post the journal entries to the ledger.	Transfer the debit and credit amounts from the journal to the ledger accounts.
4. Prepare a trial balance.	Verify that the total debits equal the total credits in the ledger.
5. Adjust the accounts.	Record adjusting entries to update the accounts for the period.
6. Prepare financial statements.	Prepare the income statement, balance sheet, and other financial statements.
7. Close the books.	Close the temporary accounts (revenues, expenses, and dividends) to the permanent accounts (retained earnings).
8. Prepare a post-closing trial balance.	Verify that the total debits equal the total credits in the ledger after closing.

Accounting cycle

Accounting cycle

- 1. Analyze the business transactions and events.
- 2. Journalize the business transactions and events.
- 3. Post the journal entries to the ledger.
- 4. Prepare a trial balance.
- 5. Adjust the accounts.
- 6. Prepare financial statements.
- 7. Close the books.
- 8. Prepare a post-closing trial balance.

Accounting cycle

- 1. Analyze the business transactions and events.
- 2. Journalize the business transactions and events.
- 3. Post the journal entries to the ledger.
- 4. Prepare a trial balance.
- 5. Adjust the accounts.
- 6. Prepare financial statements.
- 7. Close the books.
- 8. Prepare a post-closing trial balance.

Accounting cycle

Accounting cycle

- 1. Analyze the business transactions and events.
- 2. Journalize the business transactions and events.
- 3. Post the journal entries to the ledger.

Accounting cycle

- 1. Analyze the business transactions and events.
- 2. Journalize the business transactions and events.
- 3. Post the journal entries to the ledger.
- 4. Prepare a trial balance.
- 5. Adjust the accounts.
- 6. Prepare financial statements.
- 7. Close the books.
- 8. Prepare a post-closing trial balance.



Account	Debit	Credit
Accounts Receivable	1000	
Accounts Payable		500
Retained Earnings		1000
Equity		1500
Total	1000	1500

10.11. 2020/2021. évfolyam, 10. évfolyam

10.11.1. 2020/2021. évfolyam

- 10.11.1.1. 2020/2021. évfolyam
- 10.11.1.2. 2020/2021. évfolyam
- 10.11.1.3. 2020/2021. évfolyam



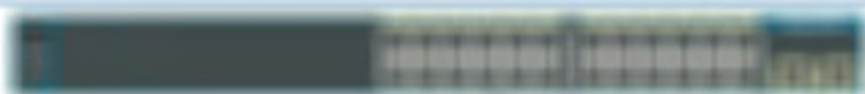
- 10.11.1.4. 2020/2021. évfolyam
- 10.11.1.5. 2020/2021. évfolyam

10.11.2. 2020/2021. évfolyam

- 10.11.2.1. 2020/2021. évfolyam
- 10.11.2.2. 2020/2021. évfolyam
- 10.11.2.3. 2020/2021. évfolyam
- 10.11.2.4. 2020/2021. évfolyam
- 10.11.2.5. 2020/2021. évfolyam
- 10.11.2.6. 2020/2021. évfolyam
- 10.11.2.7. 2020/2021. évfolyam

10.11.3. 2020/2021. évfolyam

- 10.11.3.1. 2020/2021. évfolyam
- 10.11.3.2. 2020/2021. évfolyam
- 10.11.3.3. 2020/2021. évfolyam
- 10.11.3.4. 2020/2021. évfolyam
- 10.11.3.5. 2020/2021. évfolyam
- 10.11.3.6. 2020/2021. évfolyam
- 10.11.3.7. 2020/2021. évfolyam
- 10.11.3.8. 2020/2021. évfolyam
- 10.11.3.9. 2020/2021. évfolyam
- 10.11.3.10. 2020/2021. évfolyam



10.11.4. 2020/2021. évfolyam

- 10.11.4.1. 2020/2021. évfolyam
- 10.11.4.2. 2020/2021. évfolyam



10.11.5. 2020/2021. évfolyam

- 10.11.5.1. 2020/2021. évfolyam
- 10.11.5.2. 2020/2021. évfolyam
- 10.11.5.3. 2020/2021. évfolyam
- 10.11.5.4. 2020/2021. évfolyam
- 10.11.5.5. 2020/2021. évfolyam
- 10.11.5.6. 2020/2021. évfolyam

10.11.6. 2020/2021. évfolyam

- 10.11.6.1. 2020/2021. évfolyam
- 10.11.6.2. 2020/2021. évfolyam

10.12. 2020/2021. évfolyam, 10. évfolyam

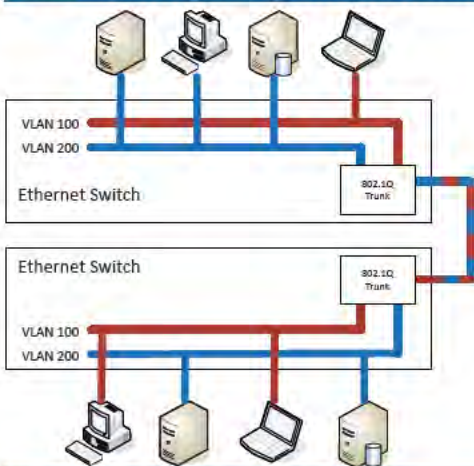
10.12.1. 2020/2021. évfolyam

- 10.12.1.1. 2020/2021. évfolyam
- 10.12.1.2. 2020/2021. évfolyam
- 10.12.1.3. 2020/2021. évfolyam
- 10.12.1.4. 2020/2021. évfolyam

10.12.2. 2020/2021. évfolyam

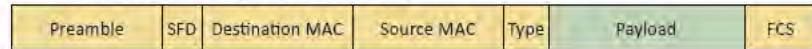
- 10.12.2.1. 2020/2021. évfolyam
- 10.12.2.2. 2020/2021. évfolyam
- 10.12.2.3. 2020/2021. évfolyam
- 10.12.2.4. 2020/2021. évfolyam
- 10.12.2.5. 2020/2021. évfolyam
- 10.12.2.6. 2020/2021. évfolyam
- 10.12.2.7. 2020/2021. évfolyam
- 10.12.2.8. 2020/2021. évfolyam
- 10.12.2.9. 2020/2021. évfolyam
- 10.12.2.10. 2020/2021. évfolyam

2.5 - Configuring Interswitch Connectivity



802.1Q trunking

- Take a normal Ethernet frame



- Add a VLAN header in the frame



- 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

1. Which of the following is a valid IPv4 address?
 A. 192.168.1.1
 B. 192.168.1.1.1
 C. 192.168.1.1.0
 D. 192.168.1.1.0.0

2. Which of the following is a valid IPv4 address?
 A. 192.168.1.1
 B. 192.168.1.1.1
 C. 192.168.1.1.0
 D. 192.168.1.1.0.0

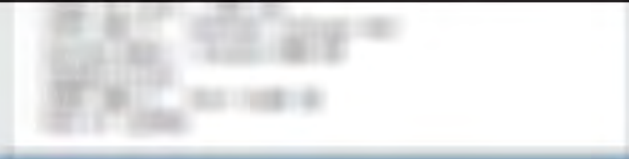
3. Which of the following is a valid IPv4 address?
 A. 192.168.1.1
 B. 192.168.1.1.1
 C. 192.168.1.1.0
 D. 192.168.1.1.0.0

4. Which of the following is a valid IPv4 address?
 A. 192.168.1.1
 B. 192.168.1.1.1
 C. 192.168.1.1.0
 D. 192.168.1.1.0.0



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

5. Which of the following is a valid IPv4 address?
 A. 192.168.1.1
 B. 192.168.1.1.1
 C. 192.168.1.1.0
 D. 192.168.1.1.0.0



6. Which of the following is a valid IPv4 address?
 A. 192.168.1.1
 B. 192.168.1.1.1
 C. 192.168.1.1.0
 D. 192.168.1.1.0.0

7. Which of the following is a valid IPv4 address?
 A. 192.168.1.1
 B. 192.168.1.1.1
 C. 192.168.1.1.0
 D. 192.168.1.1.0.0

8. Which of the following is a valid IPv4 address?
 A. 192.168.1.1
 B. 192.168.1.1.1
 C. 192.168.1.1.0
 D. 192.168.1.1.0.0

9. Which of the following is a valid IPv4 address?
 A. 192.168.1.1
 B. 192.168.1.1.1
 C. 192.168.1.1.0
 D. 192.168.1.1.0.0

Derivations of the distributive law

- $x + (y \cdot z) = (x + y) \cdot z$ (Distributive Law)
- $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ (Distributive Law)
- $x + (y \cdot z) = (x + y) \cdot z$ (Distributive Law)
- $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ (Distributive Law)
- $x + (y \cdot z) = (x + y) \cdot z$ (Distributive Law)
- $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ (Distributive Law)

$$\begin{aligned}
 &x + (y \cdot z) = (x + y) \cdot z \\
 &= (x + y) \cdot z \\
 &= (x + y) \cdot z \\
 &= (x + y) \cdot z \\
 &= (x + y) \cdot z \\
 &= (x + y) \cdot z \\
 &= (x + y) \cdot z
 \end{aligned}$$

Derivations of the distributive law

- $x + (y \cdot z) = (x + y) \cdot z$ (Distributive Law)
- $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ (Distributive Law)
- $x + (y \cdot z) = (x + y) \cdot z$ (Distributive Law)
- $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ (Distributive Law)

Derivations of the distributive law

$x + (y \cdot z) = (x + y) \cdot z$ (Distributive Law)

$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ (Distributive Law)

$x + (y \cdot z) = (x + y) \cdot z$ (Distributive Law)

$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ (Distributive Law)

Derivations of the distributive law

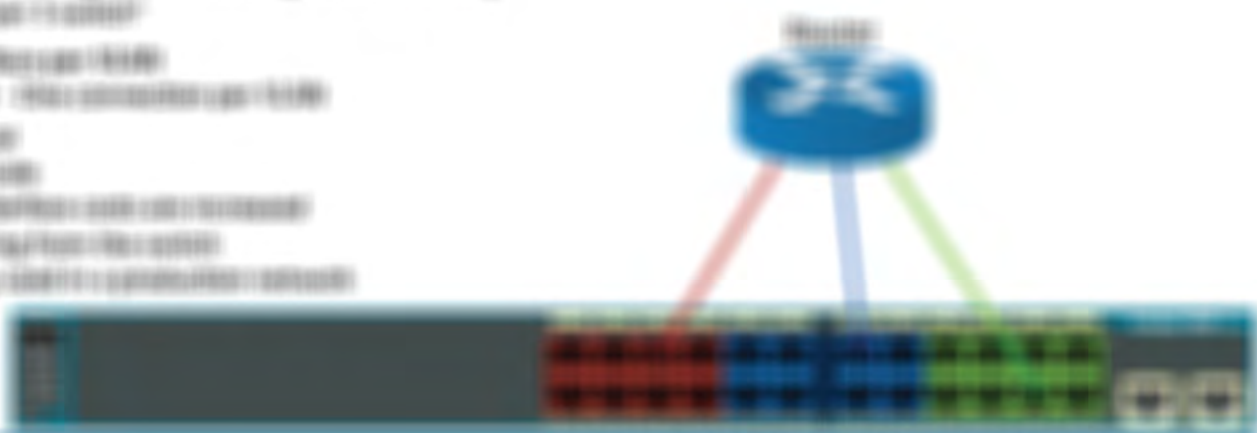
- $x + (y \cdot z) = (x + y) \cdot z$ (Distributive Law)
- $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ (Distributive Law)
- $x + (y \cdot z) = (x + y) \cdot z$ (Distributive Law)
- $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ (Distributive Law)
- $x + (y \cdot z) = (x + y) \cdot z$ (Distributive Law)
- $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ (Distributive Law)
- $x + (y \cdot z) = (x + y) \cdot z$ (Distributive Law)
- $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ (Distributive Law)
- $x + (y \cdot z) = (x + y) \cdot z$ (Distributive Law)
- $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ (Distributive Law)

Network Configuration

- 1. Configure the network interface cards (NICs) on the switches.
- 2. Configure the IP addresses on the switches.
- 3. Configure the VLANs on the switches.
- 4. Configure the inter-VLAN routing on the switches.
- 5. Configure the static routes on the switches.
- 6. Configure the dynamic routing protocols on the switches.
- 7. Configure the network security on the switches.
- 8. Configure the network monitoring on the switches.

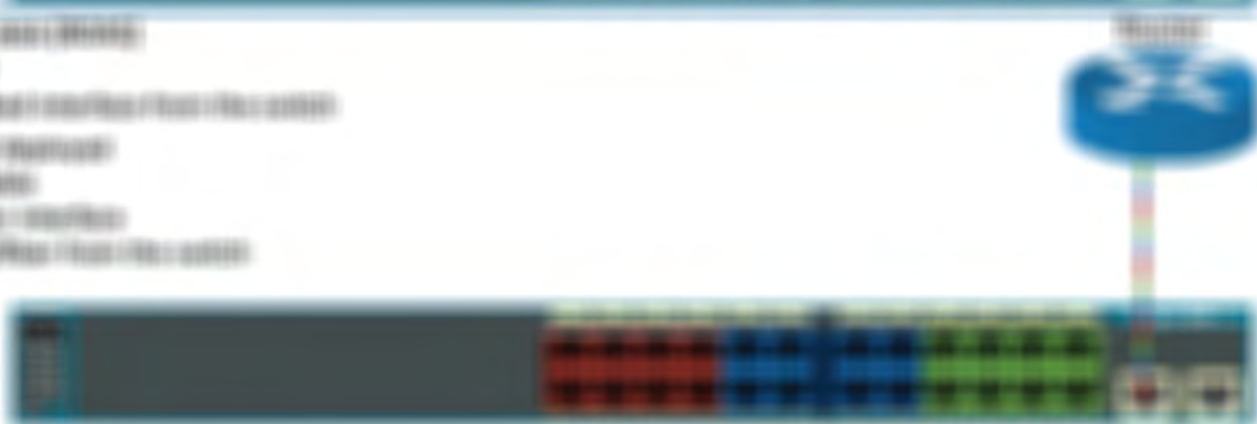
Network Configuration

- 1. Configure the network interface cards (NICs) on the switches.
- 2. Configure the IP addresses on the switches.
- 3. Configure the VLANs on the switches.
- 4. Configure the inter-VLAN routing on the switches.
- 5. Configure the static routes on the switches.
- 6. Configure the dynamic routing protocols on the switches.



Network Configuration

- 1. Configure the network interface cards (NICs) on the switches.
- 2. Configure the IP addresses on the switches.
- 3. Configure the VLANs on the switches.
- 4. Configure the inter-VLAN routing on the switches.
- 5. Configure the static routes on the switches.
- 6. Configure the dynamic routing protocols on the switches.



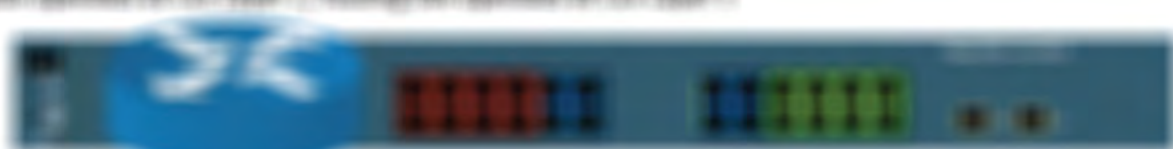
Network Configuration

- 1. Configure the network interface cards (NICs) on the switches.
- 2. Configure the IP addresses on the switches.
- 3. Configure the VLANs on the switches.
- 4. Configure the inter-VLAN routing on the switches.
- 5. Configure the static routes on the switches.
- 6. Configure the dynamic routing protocols on the switches.



Network Configuration

- 1. Configure the network interface cards (NICs) on the switches.
- 2. Configure the IP addresses on the switches.
- 3. Configure the VLANs on the switches.
- 4. Configure the inter-VLAN routing on the switches.
- 5. Configure the static routes on the switches.
- 6. Configure the dynamic routing protocols on the switches.



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
```


ICND1 - IPv4 - Routing - Summary

Topic	Pages
Introduction to IPv4	1
IPv4 Addressing	2
Routing	3
OSPF	4
EIGRP	5
RIP	6
Static Routing	7
Default Gateway	8
Networks and Subnets	9
Summary	10

ICND1 - IPv4 - Routing

Topic	Pages
Introduction to IPv4	1
IPv4 Addressing	2
Routing	3
OSPF	4
EIGRP	5
RIP	6
Static Routing	7
Default Gateway	8
Networks and Subnets	9
Summary	10

There's a lot more right here:
<http://www.professormesser.com/icnd1>

Introduction to IPv4	1
IPv4 Addressing	2
Routing	3
OSPF	4
EIGRP	5
RIP	6
Static Routing	7
Default Gateway	8
Networks and Subnets	9
Summary	10

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
 - RIPvng (RIP next generation)

Which routing protocol to use?

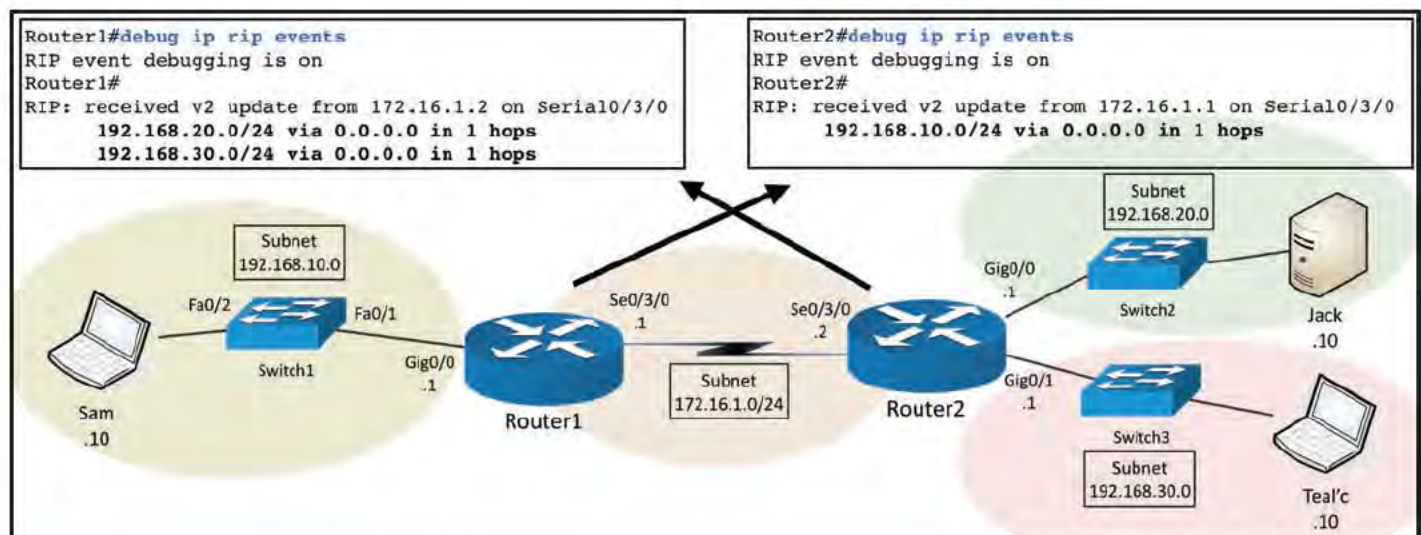
- What exactly is a route?
 - Is it based on the state of the link?
 - Is it based on how far away it is?
- How does the protocol determine the best path?
 - Some formula is applied to the criteria to create a metric
 - Rank the routes from best to worst
- Recover after a change to the network
 - Convergence 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



10.11. 1999. évi törvény a köznevelésről

- 1999. évi törvény a köznevelésről
- 1999. évi törvény a köznevelésről
- 1999. évi törvény a köznevelésről
- 1999. évi törvény a köznevelésről
- 1999. évi törvény a köznevelésről
- 1999. évi törvény a köznevelésről
- 1999. évi törvény a köznevelésről
- 1999. évi törvény a köznevelésről

- 1999. évi törvény a köznevelésről
- 1999. évi törvény a köznevelésről
- 1999. évi törvény a köznevelésről
- 1999. évi törvény a köznevelésről
- 1999. évi törvény a köznevelésről
- 1999. évi törvény a köznevelésről
- 1999. évi törvény a köznevelésről
- 1999. évi törvény a köznevelésről

10.12. 2005. évi törvény a köznevelésről

- 2005. évi törvény a köznevelésről
- 2005. évi törvény a köznevelésről
- 2005. évi törvény a köznevelésről
- 2005. évi törvény a köznevelésről
- 2005. évi törvény a köznevelésről
- 2005. évi törvény a köznevelésről
- 2005. évi törvény a köznevelésről
- 2005. évi törvény a köznevelésről

- 2005. évi törvény a köznevelésről
- 2005. évi törvény a köznevelésről
- 2005. évi törvény a köznevelésről
- 2005. évi törvény a köznevelésről
- 2005. évi törvény a köznevelésről
- 2005. évi törvény a köznevelésről
- 2005. évi törvény a köznevelésről
- 2005. évi törvény a köznevelésről

10.13. 2011. évi törvény a köznevelésről

- 2011. évi törvény a köznevelésről
- 2011. évi törvény a köznevelésről
- 2011. évi törvény a köznevelésről
- 2011. évi törvény a köznevelésről
- 2011. évi törvény a köznevelésről
- 2011. évi törvény a köznevelésről
- 2011. évi törvény a köznevelésről
- 2011. évi törvény a köznevelésről

10.14. 2011. évi törvény a köznevelésről

Államháztartás	1999-2004	2005-2010
Államháztartás	100	100
Magán	0	0
Magán	0	0
Magán	0	0

10.15. 2011. évi törvény a köznevelésről

Államháztartás	1999-2004	2005-2010
Államháztartás	100	100
Magán	0	0
Magán	0	0
Magán	0	0



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

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

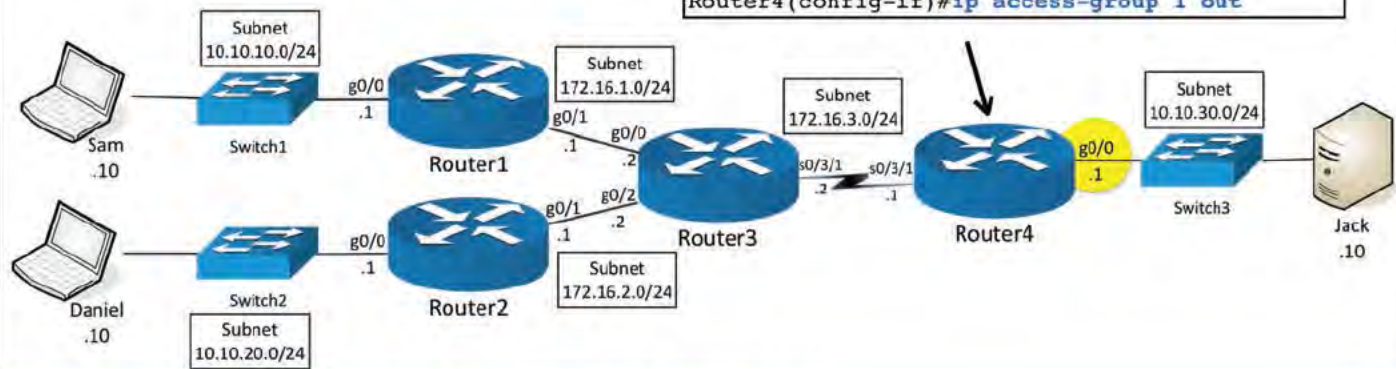
- Choose router interface and direction
  - Put a standard ACL near the destination IP - prevents inadvertent discards
  - Use the Source IP address - make sure to use the correct direction
- Create the ACLs using global configuration commands
  - Top-down matching - default is to deny if nothing else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



## 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

### 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
```

### IP Header

|                        |               |                 |                 |
|------------------------|---------------|-----------------|-----------------|
| 4 bytes                |               |                 |                 |
| Version                | Header Length | Type of Service | Total Length    |
| Identification         |               | Flags           | Fragment Offset |
| Time to Live           | Protocol      | Header Checksum |                 |
| Source IP Address      |               |                 |                 |
| Destination IP Address |               |                 |                 |
| Options and Padding    |               |                 |                 |





## 01. Configuring Network Switches and Routers



### 02. Switches

- Connect devices on a network
- Forward data packets
- Manage traffic flow
- Provide security

- Operate at Layer 2 of the OSI model
- Use MAC addresses for identification
- Support VLANs for segmentation
- Enable port security

## 03. Configuring Network Switches

- Access configuration mode
- Configure basic settings
- Set IP address
- Configure ports
- Enable port security
- Configure VLANs
- Set up Spanning Tree Protocol (STP)
- Configure security features
- Save configuration

- Access configuration mode
- Configure basic settings
- Set IP address
- Configure ports
- Enable port security
- Configure VLANs
- Set up Spanning Tree Protocol (STP)
- Configure security features
- Save configuration

### 04. Routers

- Connect different networks
- Forward data packets
- Manage traffic flow
- Provide security
- Configure interfaces
- Set up routing protocols
- Configure security features
- Save configuration

- Operate at Layer 3 of the OSI model
- Use IP addresses for identification
- Support multiple protocols
- Enable NAT for translation
- Configure security features
- Save configuration

**05. Troubleshooting Network Issues**

When troubleshooting network issues, it is important to follow a systematic approach. This includes checking physical connections, verifying IP configurations, and testing connectivity between devices. Common issues include network congestion, misconfigured settings, and hardware failures. Documenting the steps taken and the results can help in identifying the root cause of the problem.





**10.11.2019 14:17:11 - 10.11.2019 14:17:11**

- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11

- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11

**10.11.2019 14:17:11 - 10.11.2019 14:17:11**

- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11

| 10.11.2019 14:17:11 | 10.11.2019 14:17:11 | 10.11.2019 14:17:11 | 10.11.2019 14:17:11 | 10.11.2019 14:17:11 |
|---------------------|---------------------|---------------------|---------------------|---------------------|
| 10.11.2019 14:17:11 | 10.11.2019 14:17:11 | 10.11.2019 14:17:11 | 10.11.2019 14:17:11 | 10.11.2019 14:17:11 |
| 10.11.2019 14:17:11 | 10.11.2019 14:17:11 | 10.11.2019 14:17:11 | 10.11.2019 14:17:11 | 10.11.2019 14:17:11 |
| 10.11.2019 14:17:11 | 10.11.2019 14:17:11 | 10.11.2019 14:17:11 | 10.11.2019 14:17:11 | 10.11.2019 14:17:11 |

**10.11.2019 14:17:11 - 10.11.2019 14:17:11**

- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11

**10.11.2019 14:17:11 - 10.11.2019 14:17:11**

- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11



**10.11.2019 14:17:11 - 10.11.2019 14:17:11**

- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11

**10.11.2019 14:17:11 - 10.11.2019 14:17:11**

- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11
- 10.11.2019 14:17:11 - 10.11.2019 14:17:11

**6.11. Configuration Overview: Network Topologies**

- Configuration Overview: Network Topologies
- Network Topology: Simple
- Network Topology: Intermediate
- Network Topology: Complex
- Network Topology: Redundant
- Network Topology: Hierarchical

| Network Topology | Network Topology |
|------------------|------------------|
| Simple           | Intermediate     |
| Intermediate     | Complex          |
| Complex          | Redundant        |



```

 show ip route

 10.10.10.1/24 is variably subnetted, 2 subnets, 2 masks
 O 10.10.10.1/24 [120/20] via 10.10.10.254, Ethernet0/24
 O 10.10.10.2/24 [120/20] via 10.10.10.254, Ethernet0/24

```

| Network Topology | Network Topology | Network Topology | Network Topology |
|------------------|------------------|------------------|------------------|
| Simple           | Intermediate     | Complex          | Redundant        |
| Intermediate     | Complex          | Redundant        | Hierarchical     |
| Complex          | Redundant        | Hierarchical     | Other            |

- Configuration Overview: Network Topologies
- Network Topology: Simple
- Network Topology: Intermediate
- Network Topology: Complex
- Network Topology: Redundant
- Network Topology: Hierarchical
- Network Topology: Other
- Network Topology: Hybrid
- Network Topology: Mesh
- Network Topology: Ring
- Network Topology: Star
- Network Topology: Bus



Configuring DHCP

```

DHCP Pool

network 10.10.10.0/24
default-router 10.10.10.1
}

interface GigabitEthernet0/24
dhcp pool
}

```

**Configuring DHCP**  
 1. Create a DHCP pool  
 2. Configure the DHCP pool  
 3. Apply the DHCP pool to the interface

- 1. Create a DHCP pool
- 2. Configure the DHCP pool
- 3. Apply the DHCP pool to the interface
- 4. Verify the DHCP configuration
- 5. Troubleshoot DHCP issues
- 6. DHCP pool configuration
- 7. DHCP pool configuration
- 8. DHCP pool configuration

Configuring DHCP

```

DHCP Pool

network 10.10.10.0/24
default-router 10.10.10.1
}

interface GigabitEthernet0/24
dhcp pool
}

```

**Configuring DHCP**  
 1. Create a DHCP pool  
 2. Configure the DHCP pool  
 3. Apply the DHCP pool to the interface

## 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
```









## 5.3. Konfigurationsverfahren

- Handmade**
- ☐ Einzelne Konfigurationen für einzelne Netzwerke
  - ☐ Für die Netzwerke von einem zentralen Server
  - ☐ Konfigurationen werden auf den Server kopiert
  - ☐ Konfigurationen werden auf den Server kopiert
- ☐ Bei einem Fehler muss die Konfiguration manuell wieder erstellt werden
- ☐ Konfigurationen werden auf den Server kopiert
  - ☐ Konfigurationen werden auf den Server kopiert

- Konfigurations-Server**
- ☐ Konfigurationen werden von einem zentralen Server erstellt
  - ☐ Konfigurationen werden auf den Server kopiert
  - ☐ Konfigurationen werden auf den Server kopiert
  - ☐ Konfigurationen werden auf den Server kopiert

- Konfigurations-Server**
- ☐ Konfigurationen werden von einem zentralen Server erstellt
  - ☐ Konfigurationen werden auf den Server kopiert
  - ☐ Konfigurationen werden auf den Server kopiert
  - ☐ Konfigurationen werden auf den Server kopiert

```

 interface GigabitEthernet0/24
 !
 ip address 10.10.10.1 255.255.255.0
 !
 ip nat outside
 !
 ip nat pool NAT-Pool 10.10.10.1 10.10.10.254
 !
 ip nat inside source static 10.10.10.1 10.10.10.1

```

## 5.4. Konfigurations-Server

- Handmade**
- ☐ Einzelne Konfigurationen für einzelne Netzwerke
  - ☐ Konfigurationen werden auf den Server kopiert
  - ☐ Konfigurationen werden auf den Server kopiert

- ☐ Konfigurationen werden auf den Server kopiert
- ☐ Konfigurationen werden auf den Server kopiert
- ☐ Konfigurationen werden auf den Server kopiert

- Konfigurations-Server**
- ☐ Konfigurationen werden von einem zentralen Server erstellt
  - ☐ Konfigurationen werden auf den Server kopiert
  - ☐ Konfigurationen werden auf den Server kopiert





## 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 device 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 - Asynchronous 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 sgl
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
```



Table with multiple columns and rows, likely a list of items or a data table. The text is heavily blurred and illegible.

See the entire book:  
<http://www.professormesser.com/icnd1>

Table with multiple columns and rows, likely a list of items or a data table. The text is heavily blurred and illegible.





|                                                                |                            |
|----------------------------------------------------------------|----------------------------|
| Business - IT system/ processes                                | IT system/ processes/ data |
| IT system/ processes/ processes/ systems/ IT system/ processes | IT system/ processes/ data |
| IT system/ processes/ data/ systems                            | IT system/ processes/ data |
| IT system/ processes/ data/ systems/ IT system/ processes      | IT system/ processes/ data |
| IT system/ processes/ data/ systems/ IT system/ processes      | IT system/ processes/ data |
| IT system/ processes/ data/ systems/ IT system/ processes      | IT system/ processes/ data |
| IT system/ processes/ data/ systems/ IT system/ processes      | IT system/ processes/ data |
| IT system/ processes/ data/ systems/ IT system/ processes      | IT system/ processes/ data |
| IT system/ processes/ data/ systems/ IT system/ processes      | IT system/ processes/ data |
| IT system/ processes/ data/ systems/ IT system/ processes      | IT system/ processes/ data |
| IT system/ processes/ data/ systems/ IT system/ processes      | IT system/ processes/ data |
| IT system/ processes/ data/ systems/ IT system/ processes      | IT system/ processes/ data |
| IT system/ processes/ data/ systems/ IT system/ processes      | IT system/ processes/ data |
| IT system/ processes/ data/ systems/ IT system/ processes      | IT system/ processes/ data |

```

Business Systems Theory - a system of ideas, concepts, models, and processes, which are used to describe, explain, and predict the behaviour of organisations.

Business Systems Theory - a system of ideas, concepts, models, and processes, which are used to describe, explain, and predict the behaviour of organisations.

Business Systems Theory - a system of ideas, concepts, models, and processes, which are used to describe, explain, and predict the behaviour of organisations.

Business Systems Theory - a system of ideas, concepts, models, and processes, which are used to describe, explain, and predict the behaviour of organisations.

Business Systems Theory - a system of ideas, concepts, models, and processes, which are used to describe, explain, and predict the behaviour of organisations.

```

|                                                                |                            |
|----------------------------------------------------------------|----------------------------|
| Business - IT system/ processes                                | IT system/ processes/ data |
| IT system/ processes/ processes/ systems/ IT system/ processes | IT system/ processes/ data |
| IT system/ processes/ data/ systems                            | IT system/ processes/ data |
| IT system/ processes/ data/ systems/ IT system/ processes      | IT system/ processes/ data |
| IT system/ processes/ data/ systems/ IT system/ processes      | IT system/ processes/ data |
| IT system/ processes/ data/ systems/ IT system/ processes      | IT system/ processes/ data |
| IT system/ processes/ data/ systems/ IT system/ processes      | IT system/ processes/ data |
| IT system/ processes/ data/ systems/ IT system/ processes      | IT system/ processes/ data |
| IT system/ processes/ data/ systems/ IT system/ processes      | IT system/ processes/ data |
| IT system/ processes/ data/ systems/ IT system/ processes      | IT system/ processes/ data |
| IT system/ processes/ data/ systems/ IT system/ processes      | IT system/ processes/ data |
| IT system/ processes/ data/ systems/ IT system/ processes      | IT system/ processes/ data |
| IT system/ processes/ data/ systems/ IT system/ processes      | IT system/ processes/ data |
| IT system/ processes/ data/ systems/ IT system/ processes      | IT system/ processes/ data |
| IT system/ processes/ data/ systems/ IT system/ processes      | IT system/ processes/ data |

1. Schritt: ...  
2. Schritt: ...  
3. Schritt: ...

4. Schritt: ...  
5. Schritt: ...

6. Schritt: ...  
7. Schritt: ...

8. Schritt: ...  
9. Schritt: ...

10. Schritt: ...

11. Schritt: ...  
12. Schritt: ...

13. Schritt: ...

14. Schritt: ...  
15. Schritt: ...

16. Schritt: ...

17. Schritt: ...

18. Schritt: ...

19. Schritt: ...

20. Schritt: ...

21. Schritt: ...

22. Schritt: ...  
23. Schritt: ...  
24. Schritt: ...

25. Schritt: ...

26. Schritt: ...

27. Schritt: ...

28. Schritt: ...

29. Schritt: ...  
30. Schritt: ...  
31. Schritt: ...

32. Schritt: ...

33. Schritt: ...

34. Schritt: ...

35. Schritt: ...

36. Schritt: ...

37. Schritt: ...  
38. Schritt: ...  
39. Schritt: ...



## 11.12: Transmittanzmessung mit TSP

**Wiss:**

- 1. Bestimmung der Transmittanz (T) als Funktion der Schichtdicke (d) und der Extinktion (k):  $T = e^{-kd}$
- 2. Zusammenhang zwischen Transmittanz (T) und Absorption (A):  $A = -\log_{10}(T) = \log_{10}(1/T)$
- 3. Bestimmung der Extinktion (k) aus dem Absorptionskoeffizienten (k<sub>ext</sub>):  $k = k_{ext} \cdot c$
- 4. Zusammenhang zwischen Extinktion (k) und der Konzentration (c) des Kolloids:  $k = k_{ext} \cdot c$
- 5. Bestimmung der Konzentration (c) des Kolloids aus der Extinktion (k):  $c = k / k_{ext}$

**Wiss (Zusammenfassung):**

- 1. Bestimmung der Transmittanz (T) als Funktion der Schichtdicke (d) und der Extinktion (k):  $T = e^{-kd}$
- 2. Zusammenhang zwischen Transmittanz (T) und Absorption (A):  $A = -\log_{10}(T) = \log_{10}(1/T)$
- 3. Bestimmung der Extinktion (k) aus dem Absorptionskoeffizienten (k<sub>ext</sub>):  $k = k_{ext} \cdot c$
- 4. Zusammenhang zwischen Extinktion (k) und der Konzentration (c) des Kolloids:  $k = k_{ext} \cdot c$
- 5. Bestimmung der Konzentration (c) des Kolloids aus der Extinktion (k):  $c = k / k_{ext}$

## 11.13: Transmittanzmessung mit Transmittanz

**Wiss:**

- 1. Bestimmung der Transmittanz (T) als Funktion der Schichtdicke (d) und der Extinktion (k):  $T = e^{-kd}$
- 2. Zusammenhang zwischen Transmittanz (T) und Absorption (A):  $A = -\log_{10}(T) = \log_{10}(1/T)$
- 3. Bestimmung der Extinktion (k) aus dem Absorptionskoeffizienten (k<sub>ext</sub>):  $k = k_{ext} \cdot c$
- 4. Zusammenhang zwischen Extinktion (k) und der Konzentration (c) des Kolloids:  $k = k_{ext} \cdot c$
- 5. Bestimmung der Konzentration (c) des Kolloids aus der Extinktion (k):  $c = k / k_{ext}$



**Wiss (Zusammenfassung):**

- 1. Bestimmung der Transmittanz (T) als Funktion der Schichtdicke (d) und der Extinktion (k):  $T = e^{-kd}$
- 2. Zusammenhang zwischen Transmittanz (T) und Absorption (A):  $A = -\log_{10}(T) = \log_{10}(1/T)$
- 3. Bestimmung der Extinktion (k) aus dem Absorptionskoeffizienten (k<sub>ext</sub>):  $k = k_{ext} \cdot c$
- 4. Zusammenhang zwischen Extinktion (k) und der Konzentration (c) des Kolloids:  $k = k_{ext} \cdot c$
- 5. Bestimmung der Konzentration (c) des Kolloids aus der Extinktion (k):  $c = k / k_{ext}$

**Wiss (Zusammenfassung):**

- 1. Bestimmung der Transmittanz (T) als Funktion der Schichtdicke (d) und der Extinktion (k):  $T = e^{-kd}$
- 2. Zusammenhang zwischen Transmittanz (T) und Absorption (A):  $A = -\log_{10}(T) = \log_{10}(1/T)$
- 3. Bestimmung der Extinktion (k) aus dem Absorptionskoeffizienten (k<sub>ext</sub>):  $k = k_{ext} \cdot c$
- 4. Zusammenhang zwischen Extinktion (k) und der Konzentration (c) des Kolloids:  $k = k_{ext} \cdot c$
- 5. Bestimmung der Konzentration (c) des Kolloids aus der Extinktion (k):  $c = k / k_{ext}$



**Wiss (Zusammenfassung):**

- 1. Bestimmung der Transmittanz (T) als Funktion der Schichtdicke (d) und der Extinktion (k):  $T = e^{-kd}$
- 2. Zusammenhang zwischen Transmittanz (T) und Absorption (A):  $A = -\log_{10}(T) = \log_{10}(1/T)$
- 3. Bestimmung der Extinktion (k) aus dem Absorptionskoeffizienten (k<sub>ext</sub>):  $k = k_{ext} \cdot c$
- 4. Zusammenhang zwischen Extinktion (k) und der Konzentration (c) des Kolloids:  $k = k_{ext} \cdot c$
- 5. Bestimmung der Konzentration (c) des Kolloids aus der Extinktion (k):  $c = k / k_{ext}$

## 11.14: Messung der Konzentration

**Wiss:**

- 1. Bestimmung der Konzentration (c) des Kolloids aus der Extinktion (k):  $c = k / k_{ext}$
- 2. Zusammenhang zwischen Extinktion (k) und der Konzentration (c) des Kolloids:  $k = k_{ext} \cdot c$
- 3. Bestimmung der Konzentration (c) des Kolloids aus der Extinktion (k):  $c = k / k_{ext}$

**Wiss (Zusammenfassung):**

- 1. Bestimmung der Konzentration (c) des Kolloids aus der Extinktion (k):  $c = k / k_{ext}$
- 2. Zusammenhang zwischen Extinktion (k) und der Konzentration (c) des Kolloids:  $k = k_{ext} \cdot c$
- 3. Bestimmung der Konzentration (c) des Kolloids aus der Extinktion (k):  $c = k / k_{ext}$

## 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`

### 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`

| 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               |



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

**<http://www.professormesser.com/icnd1>**





# 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>