# CCNA 2

# LAN Design

## Converged Networks

### Borderless Switched Networks

Architecture to allow organizations to connect to anyone, anywhere at any time on any device securely, reliably and seamlessly.

### BSN principle: Hierarchy

* **Hierarchical:** Understanding the role of each device at every tier
* **Modularity:** Seamless network expansion
* **Resiliency:** Network always on
* **Flexibility:** Intelligent traffic load sharing by using all network resources

### Core Distribution Access

* **Access Layer:** Network edge -> Network access to user
* **Distribution Layer:** Interfaces between Access and Core Layer
* **Core Layer:** Network Backbone, connects campus together

## Switched Networks

### Role of Switched Networks

* **Quality of Service**
* **Additional Security**
* **Wireless networking & connectivity**
* **New technologies:** IP telephony & mobility services

### Form Factors

* **Cost:** Price of switch depends on number & speed of interfaces, supported features & expansion capability
* **Port Density:** Network switches must support amount of devices
* **Power: PoE (**Power over Ethernet**)**
* **Reliability:** Continuous access to the network
* **Frame Buffers:** Ability to store frames
* **Scalability:** Users on a network typically grow over time
* **Fixed Configuration Switches:** No feature support other than original.
* **Modular Configuration Switches:** Allow modular line cards for more features
* **Stackable Configuration Switches:** Connect switches with high bandwidth cable. (Up to 9)

## The Switched Environment

### Frame Forwarding

#### Dynamically Populating switch MAC address table

* Populates table based on source addresses.
* If incoming frame destination MAC is not found -> Flood

### Switch Forwarding Methods

#### Store-and-Forward Switching

Receives entire frame (+ CRC check). Looks up destination address and forwards to correct port.

* **Error Checking:** FCS (Frame check sequence), if false, frame is dropped.
* **Automatic Buffering:** Flexibility to support mix of Ethernet speeds.

#### Cut-Through Switching

Forwards frame before entirely received. Minimum: Destination address needed.

* **Rapid Frame Forwarding:** No wait time
* **Fragment Free:** Modified form of Cut-through:
  + Waits for collision window (64 bytes)
  + Makes sure no fragmentation has occurred

## Switching Domains

### Collision Domains

Network segments that share the same bandwidth between devices.  
Two or more devices within the segment may try to communicate at the same time -> Collision.

By using switches or routers, you can divide a network into segments and reduce the number of devices that compete for bandwidth.

### Broadcast Domains

A collection of interconnected switches forms a broadcast domain. = MAC broadcast domain.

### Alleviating Network Congestion

LAN switches have special characteristics that make them effective at alleviating network congestion.

* Allow segmentation of LAN is separate collision domains, each port = collision domain
* Full duplex communication between devices
* **High Port Density:** 24-48 port switches are often 1 rack & operate at 100mb-10Gb/s
* **Large frame buffers**
* **Port Speed**
* **Fast internal switching**
* **Low per-port cost**

# Basic Switching Concepts and Configuration

## Configure a Switch with initial settings

### Switch Boot Sequence

1. **Power-on self-test (POST):** Stored in ROM. Tests CPU, DRAM and flash file system.
2. **Load bootloader software:** Small program stored in ROM.
3. **CPU initialization by bootloader:** CPU registers, which control where physical memory is mapped, quantity & speed.
4. **Flash File System initialization by bootloader**
5. **Bootloader loads IOS and gives control:** Boot environment table or first executable file

### Recovering from a system crash

The bootloader has a command-line that provides access to the files stored in flash memory. It can be accessed by the following steps:

1. Connect PC by console cable to the switch console port. Use terminal emulation software
2. Unplug switch power cord
3. Reconnect the power cord and press and hold down the mode button, within 15 seconds
4. Release the button until the system led briefly turns amber and then solid green
5. The software will show: “switch:”

### Switch LED indicators

* **System LED:** Receiving power (Green) & functioning properly (Amber)
* **Redundant Power System (RPS) LED:** RPS status
* **Port Status LED:** Off – Down, Green – link, blink green – activity, green-amber – link fault, amber – blocked, blink amber – blocked to prevent possible loop in forwarding domain.
* **Port Duplex LED:** Green if on
* **Port Speed LED:** off – 10Mb/s, Green – 100Mb/s, blink green – 1000Mb/s
* **Power over Ethernet (PoE) Mode LED**

### Preparing For Basic Switch Management

To enable remote management access, the switch must be configured with an IP address and a subnet mask. If the switch must be managed from a remote network, it must also be configured with a default gateway. This will be configured to a virtual interface. (VLAN).

### Configure Basic Switch Management Access with IPv4

1. **Configure Management Interface:**
   1. “interface vlan 99 -> ip address -> no shutdown”
   2. “vlan vlan\_id -> name vlan\_name -> end -> interface interface\_id -> switchport access vlan vlan\_id”
2. **Configure Default Gateway**
   1. If managed from remote networks
   2. “ip default-gateway”
   3. **Verify:** ‘show ip interface brief”

## Switch Security: Management and Implementation

### Secure Remote Access

#### SSH operation

SSH (Secure Shell) is a protocol that provides encrypted management connection to a remote device. It should replace Telnet, which is an older protocol that uses insecure plaintext for login and data.

#### Configuring SSH

1. **Verify SSH support:** “**show ip ssh**”
2. **Configure the IP domain:** “**ip domain-name** domain-name”
3. **Generate RSA key pairs: “ip ssh version 2**” -> “**crypto key generate rsa**”
4. **Configure user authentication:** “**username** username s**ecret** password
5. **Configure VTY lines:** “**transport input ssh**” -> “**line vty”** -> “**login local**”

### Security Concerns in LAN’s

#### Mac Address Flooding

As a frame arrives on a switch, the source address is recorded. If an entry exists for the destination address, the frame gets forwarded, if not, it gets flooded to all ports but the incoming port.

The MAC address table is limited, when it gets overwhelmed with fake source MAC addresses until the table is full, it enters a fail-open mode. The switch then broadcasts all frames to all machines on the network, as a result, the attacker can see all of the frames.

#### DHCP Spoofing

* **DHCP starvation attacks:**Attacker floods DHCP server with requests to use up all the available IP addresses. It produces a DoS attack as new devices cannot obtain network access.
* **DHCP Spoofing attacks:**  
  Attacker configures a fake DHCP server on the network, which may force the clients to use a false DNS or Windows Internet Naming Service (WINS) and make them use the attacker as default gateway.

#### Leveraging CDP

CDP (Cisco Discovery Protocol): Protocol to discover directly connected cisco devices and automatically configure the connection. Contains info about device (ip, software, native VLAN, …). This info may be used by an attacker to find ways to attack a network.

#### Telnet Attacks

Telnet is insecure and can give remote access. Tools are available to brute force the login on VTY lines.

#### Telnet DOS attack

By exploiting a flaw in the telnet server software, the telnet service can be rendered useless, preventing an administrator from using management functions. Usually combined with direct attacks in a coordinated breach.

### Security Best Practices

* Shut Down unused services & ports
* Use strong passwords and often change them
* Physical access to devices
* Use HTTPS instead of HTTP for login screens
* Perform tested backups
* Encrypt and password sensitive data
* Implement security like firewalls
* Update software regularly

#### Network Security Audits

A security audit reveals the type of information an attacker can gather simply by monitoring network traffic. Tests such as a network penetration test are made in a controlled situation, in an off-line situation.

### Switch Port Security

#### Secure Unused Ports

When a switch has for example 24 ports and only 3 are used, it’s a good practice to disable to unused ports. This can be done with the IOS “**shutdown**” command and it’s made easier with “**interface range**”

#### DHCP Snooping

A Cisco Catalyst feature to determine which switch ports can respond to DHCP requests. Trusted ports can be a DHCP server or an uplink to it. When a rogue device sends a DHCP response packet in the network, the port is shutdown.

1. **Enable DHCP snooping:** “**ip dhcp snooping (vlan** ID**)**”
2. **Define ports as trusted:** “**ip dhcp snooping trust**”
3. **Limit bogus DHCP request rate:** “**ip dhcp snooping limit rate** rate”

# VLAN Segmentation

## Overview of VLAN’s

### Definitions

VLAN’s provide segmentation and organizational flexibility. Each VLAN is considered a separate logical network and broadcast domains become smaller.

### Benefits

1. **Security:** Sensitive data is separated from the rest of the network
2. **Cost reduction:** More efficient use of existing bandwidth and uplinks
3. **Better performance:** Reduces unnecessary traffic on the network
4. **Shrink Broadcast domains**
5. **Improved IT staff efficiency:** Similar network requirements share the same VLAN
6. **Simpler project and application management:** separate functions makes managing easier

### Types

#### Data VLAN

* User Generated Traffic
* Separate Network into groups of users and devices

#### Default VLAN

* VLAN 1 = Default VLAN
* Contains all ports on initial boot
* Cannot be renamed or deleted

#### Native VLAN

* Assigned to trunk ports
* Trunk port places untagged traffic on native VLAN

#### Management VLAN

* To access management capabilities of switch
* Default VLAN 1 (= Security Risk)

#### Voice VLAN

* Assured bandwidth
* Transmission priority
* Ability to be routed around congested areas
* Less than 150ms delay

## VLAN’s in a Multi-Switched Environment

### VLAN Trunks

A VLAN trunk is a point-to-point link between two network devices that carry more than one VLAN.

### Controlling Broadcast Domains with VLAN’s

* Use Ethernet Frame Header, default header doesn’t contain info
* When placed on trunk, information gets added

A VLAN Tag Field:

* **Type:** (2 Bytes) | Tag Protocol ID (TPID)
* **User Priority:** (3 Bit) | Level or service implementation
* **Canonical Format Identifier (CFI):** (1 Bit) Identifier to enable Token Ring frames to be carries across Ethernet links
* **VLAN ID (VID):** (12 Bit) VLAN ID number that supports up to 4096 VLAN ID’s

### Native VLANs and 802.1Q Tagging

* **Tagged Frames on Native VLAN:** Some devices tag native VLAN traffic, but control traffic should not be tagged. If trunk port receives a tagged frame where VLAN ID = Native VLAN, the frame is dropped.
* **Untagged Frames on Native VLAN:** When there is no VLAN ID, the traffic is forwarded to the native VLAN.

## VLAN Implementations

### VLAN Assignment

#### VLAN Ranges on Catalyst Switches

1. **Normal Range:**

* VLAN ID: 1-1005
* Token Ring and FDDI VLANs: 1002-1005
* 1 & 1002-1005 are auto created and cannot be removed
* Config stored in vlan.dat (FLASH)

1. **Extended range VLANs:**

* Greater number of customers
* VLAN ID: 1006-4094
* No VLAN.dat, but Running Config file
* Fewer VLAN features

### Dynamic Trunking Protocol

#### Introduction to DTP

Only for cisco devices. If there’s a connected trunk port, the switch negotiates. If two connected ports are configured on auto, the trunk link is inactive.

#### Negotiated interface Modes

* **Switchport mode access:** Permanent non-trunking mode
* **Switchport mode dynamic auto:** Default, able to turn into trunk link
* **Switchport mode dynamic desirable:** Becomes trunk if neighbour is trunk, desirable or auto.
* **Switchport mode trunk:** Permanent trunking mode
* **Switchport nonegotiate:** Stops interface from generating DTP frames (only access or trunk)

### Troubleshoot VLANs and Trunks

#### IP Addressing Issues with VLAN

Each VLAN must have a unique IP subnet. If there are two devices in the same VLAN, with a different subnet, they cannot communicate.

#### Common Problems with Trunks

* **Native VLAN mismatches:** Trunk ports are configured with different native VLANS
* **Trunk mode mismatches:** One is trunk mode on, one is trunk mode off
* **Allowed VLANs on trunks:** allowed VLANs on trunk is not updated

## VLAN Security and Design

### Attacks on VLANs

#### Switch Spoofing Attack

* Pretends to be a switch with auto trunk port
* Gains access to all VLANs allowed on trunk port

### Double-Tagging Attack

* Double tagged frame
* Switch sees first tag, strips it and forwards it to corresponding VLAN
* Second switch sees original tag and floods or sends to port with corresponding MAC
* **Solution:** Native VLAN of trunk ports different that the VLAN of any user port.

### PVLAN Edge (Private VLAN)

* Protected ports do not forward traffic to other protected ports (unless control traffic)
* Forward between protected and non-protected is normal

# Initial Configuration of a Router

## Functions of a Router

### Characteristics of a Network

#### Routers are Computers

They have a CPU, OS and memory and storage:

* **RAM (Volatile):** Running IOS, Running config, IP routing & ARP tables, Packet buffer
* **ROM:** Boot up instructions, Basic Diagnostic software, Limited IOS
* **NVRAM:** Start-up Config
* **Flash:** IOS, system files

#### Packet Forwarding Mechanisms

* **Process Switching:**
  + Packet Arrives on interface
  + Packet gets forwarded to control plane
  + CPU matches destination address with entry in routing table, determines exit interface & forwards the packet
  + **Repeats for every packet, slow and rarely implemented in modern networks**
* **Fast Switching:**
  + Packet Arrives on interface
  + Packet gets forwarded to control plane
  + CPU matches destination address with fast-switching cache entry
  + If no match -> Process Switching & flow info is stored in fast-switching cache
  + If another packet going the same direction comes, no CPU intervention is needed
* **Cisco Express Forwarding (CEF)**
  + Build FIB (Forwarding Information Base) and adjacency table.
  + Entries are change triggered instead of packet triggered.
  + Contains pre-computed reverse lookups and next hop info

## Routing Decisions

### Switch Packets between Networks

#### Router Switching Function

* Forward packets to destination
* If packet from another network is destined to another network:
  + De-Encapsulate Layer3 packet by removing Layer 2 frame header and trailer
  + Examine destination IP and find best path in routing table
  + Encapsulate Layer 3 packet into new Layer 2 frame and forward to exit interface

#### Send a Packet

* Looks up MAC in ARP table by IPV4 address.
* If no entry -> ARP request

### Path Determination

#### Routing Decisions

* **Directly Connected Network:** When connected directly to an interface, it gets forwarded
* **Remote Network:** When in anther network, the packet gets forwarded to anther router
* **No route determined:** Forwarded to Gateway of Last Resort, or if none, it is discarded.

### Best Path

Dynamic protocols:

* **Routing Information Protocol (RIP):** Hop Count
* **Open Shortest Path First (OSPF):** Cisco’s cost based on cumulative bandwidth
* **Enhanced Interior Gateway Routing Protocol (EIGRP):** Bandwidth, delay, load, reliability
* **IS-IS:** Intermediate System-to-Intermediate System

### Load Balancing

If a router has two paths with identical cost metrics, the router uses both paths equally.  
Only EIGRP supports unequal cost load balancing.

### Administrative Distance

When there are multiple routing protocols configured on a router, it’s possible that there are multiple ways of reaching a destination. In order to know what route to use, Cisco IOS uses AD. The lower the number, the more trustworthy a route is.

## Router Operation

### Analyse the Routing table

#### The routing table

* **Directly connected routes:**
  + Routers add a directly connected route when an interface is configured with an ip and is activated.
* **Remote routes:**
  + Can be statically or dynamically configured
  + Default static route: 0.0.0.0 0.0.0.0/0
  + Ip route <addr> <exit in/nexthop>

#### Remote Network Routing Entries

A routing table contains following information:

* **Route source (\*):** How was the route learned
* **Destination network (\*):** address of remote network
* **Administrative distance (AD):** trustworthiness, less is better
* **Metric:** less is better
* **Next-hop:** Ipv4 Address of the next router to forward the packet to
* **Route timestamp:** time since route was learned
* **Outgoing interface (\*):** exit interface to forward packet towards final destination

**\***: Directly connected routing table entries as well.

# Inter-VLAN Routing Configuration

### What is inter-VLAN routing

* Computers on different VLANs cannot communicate
* A routing device is needed to make this possible
* **Inter-VLAN:** Forwarding Traffic between VLANs

### Legacy Inter-VLAN routing

* A router had 2 different physical interfaces, each with a separate network & distinct subnet
* By using a switch, the router could accept traffic from the VLANs associated with the switch interfaces.

### Router-on-a-stick Inter-VLAN Routing

* Single physical interface on router and switch, routes traffic between VLANs
* Router interface is configured to work as a trunk
* Routing VLANs using sub interfaces
* Maximum for 50 VLANs

### Multilayer Switch Inter-VLAN Routing

* Dedicated router not required
* Multilayer switch ip routing enabled
* More ports = more scalable
* Traffic is routed internally

## Layer 3 Switching

### Layer 3 Switching Operation and Configuration

#### Introduction to Layer 3 switching

* **Routed Port:** Layer 3 interface similar to a physical interface on Cisco router
* **Switched virtual Interface (SVI):** Virtual VLAN interface for inter-VLAN routing

#### Inter-VLAN Routing with SVI:

* Distribution Switches = Layer 3
* Layer 3 takes care of routing the VLANs

#### Inter-VLAN Routing with Routed Ports

* Routed port = physical port
* Works similarly to interface
* L2 functions don’t work

#### Configure Static routes

* **Ip route <**netw.Addr><subnet><nexthop/exitint>

# Static Routing Implementation

### Static Routing

#### Reach Remote Networks

A router can learn about remote networks in two ways:

* **Manually:** Manually enter networks in route table using static routes
* **Dynamically:** Automatically learned using a dynamic routing protocol

#### Why use Static Routing

* Not advertised on the network -> Better security
* Uses almost no bandwidth, no CPU usage
* Path used to send data is known
* Time-consuming initial configuration and maintenance
* Error-prone in larger networks
* Administrator intervention required when changing route information
* Doesn’t scale with larger networks
* Requires complete knowledge of network

#### When to use Static Routing

* Easy routing table maintenance in smaller networks
* Routing to and from stub networks (= network with only one neighbour)
* Default route for a network that does not have any more specific path

### Types of Static Routes

#### Standard Static Route

* Connecting to a specific remote network
* Mainly used for stub networks

#### Default Static Route

* Static route with 0.0.0.0/0 as destination address (=Gateway of last resort)

#### Summary Static Route

* Summarize network address to reduce routing table entries, possible if:
  + Destination networks are contiguous and can be put in single network address
  + Multiple static routes all use same exit interface or next-hop IP

#### Floating Static Route

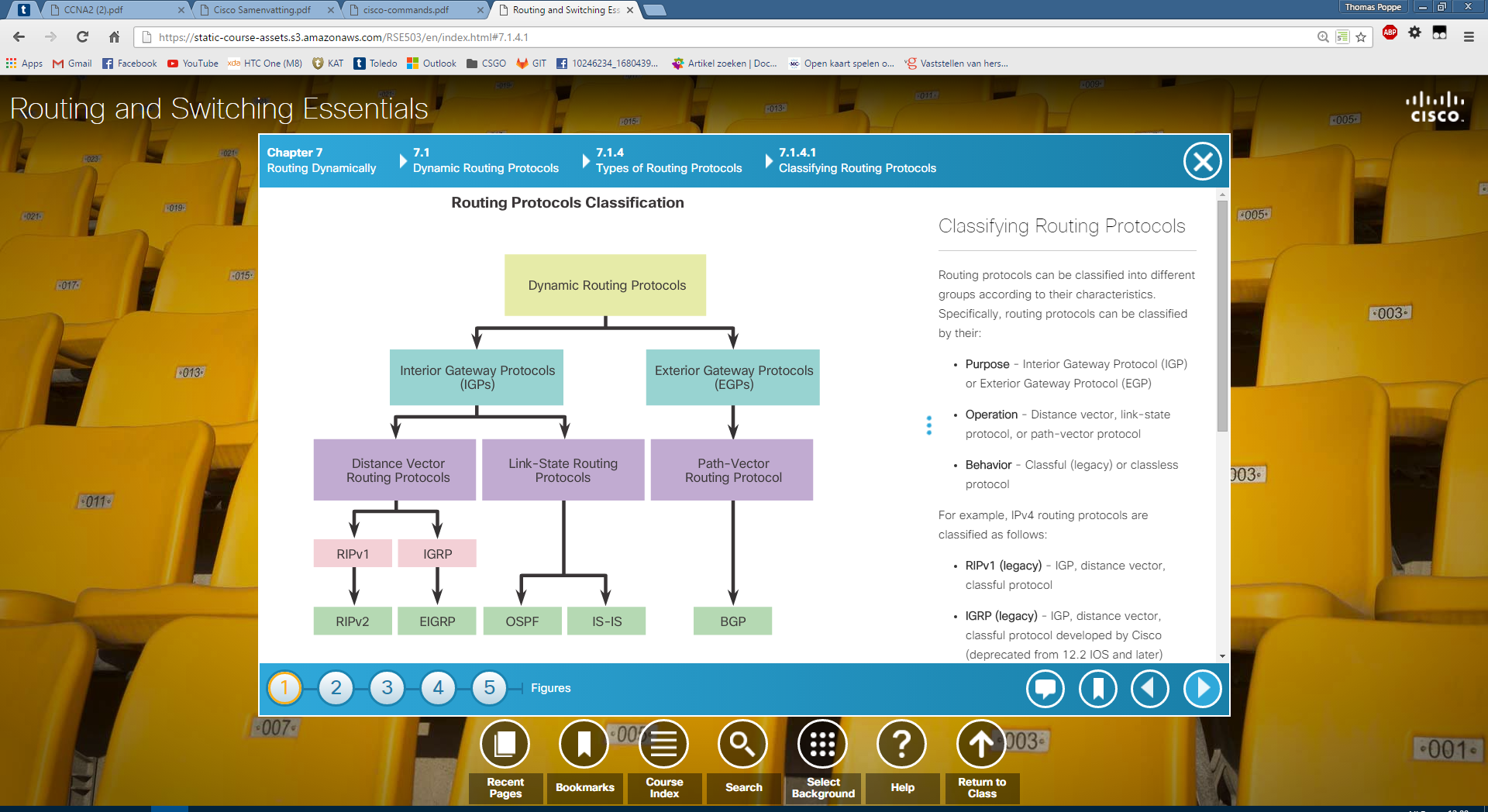
* Backup Path
* Higher administrative distance

# Dynamic Routing Protocols

## Routing Protocol Operations

* **Cold Start:** Each router has his neighbours in routing table
* **Network Discovery:** Adding neighbours in routing table
* **Exchanging the Routing Information:** Repeat Network Discovery until routing table is complete

## Types of Routing Protocols



### Distance Vector Routing Protocol

* **Routes are provided by characteristics:**
  + **Distance:** hop count, bandwidth, delay, cost …
  + **Vector:** Direction of the next-hop router or exit interface
* **Doesn’t know entire path to destination**

### Link-state routing protocols

* Can create a view of complete topology
* Complete map of network
* Update on change

## Distance Vector Dynamic Routing

### Distance Vector Routing Protocol Operation

#### Distance Vector Technology

* Update between neighbours:
  + **RIP\_V1:** Broadcast periodically
  + **RIPv2:** Multicast to neighbours that need it
  + **EIGRP:** Multicast/Unicast to neighbours that need it

#### Distance Vector Algorithm

The used algorithms are based on following processes:

* Mechanism for sending & receiving routing info
* Mechanism for calculating the best paths and installing routes in the routes table
* Mechanism for detecting and reacting to topology changes

#### Routing Information Protocol (RIP)

Version 1:

* Routing updates are broadcasted every 30 seconds
* Path selection based on hop count
* Max hop count = 15.

Version 2 included multiple improvements:

* **Classless routing protocol:** Supports VLSM & CIDR: Includes subnet masks in routing updates
* **Increased efficiency:** forwards updates to multicast address instead of broadcasting
* **Reduced routing entries:** Supports manual route summarization on any interface
* **Secure:** Supports authentication mechanism to secure routing table updates

#### Enhanced Interior-Gateway routing Protocol (EIGRP)

IGRP was introduced with following characteristics:

* Path selection based on Bandwidth, delay, load and reliability
* Routing updates are broadcasted every 90 seconds

Later it was updates as EIGRP:

* **Bound Trigger Updates:** No periodic updates: Whenever routing table change occurs
* **Hello keep alive mechanism:** Small hello message periodically sent to maintain adjacencies with neighbour routers.
* **Maintains a topology table:** Not only best paths are kept, but all are.
* **Rapid convergence:** Has backup paths
* **Multiple network layer protocol support:** Uses PDM (Protocol Dependent Modules) = Supports protocols other than IPv4 & IPv6

## Link-State Dynamic Routing

### Link-State Routing Protocol Operation

Link state protocols are known as shortest path first protocols. They are more complex than distance vector protocols.

There are two main protocols for IPv4:

* **OSPF:** Open Shortest Path Frist
* **IS-IS:** Intermediate System-To-Intermediate System

### Link-State Routing Protocol Process

1. Each router learns own links and directly connected networks.
2. Each router exchanges Hello packets with other link-state routers to meet its neighbours.
3. Each router builds a Link-State Packet (LSP): Contains state of each directly connected link.
4. Each router floods LSP to all neighbours, which store it in a database and flood it as well.
5. Each router uses the database to create a map topology and computes the best paths.

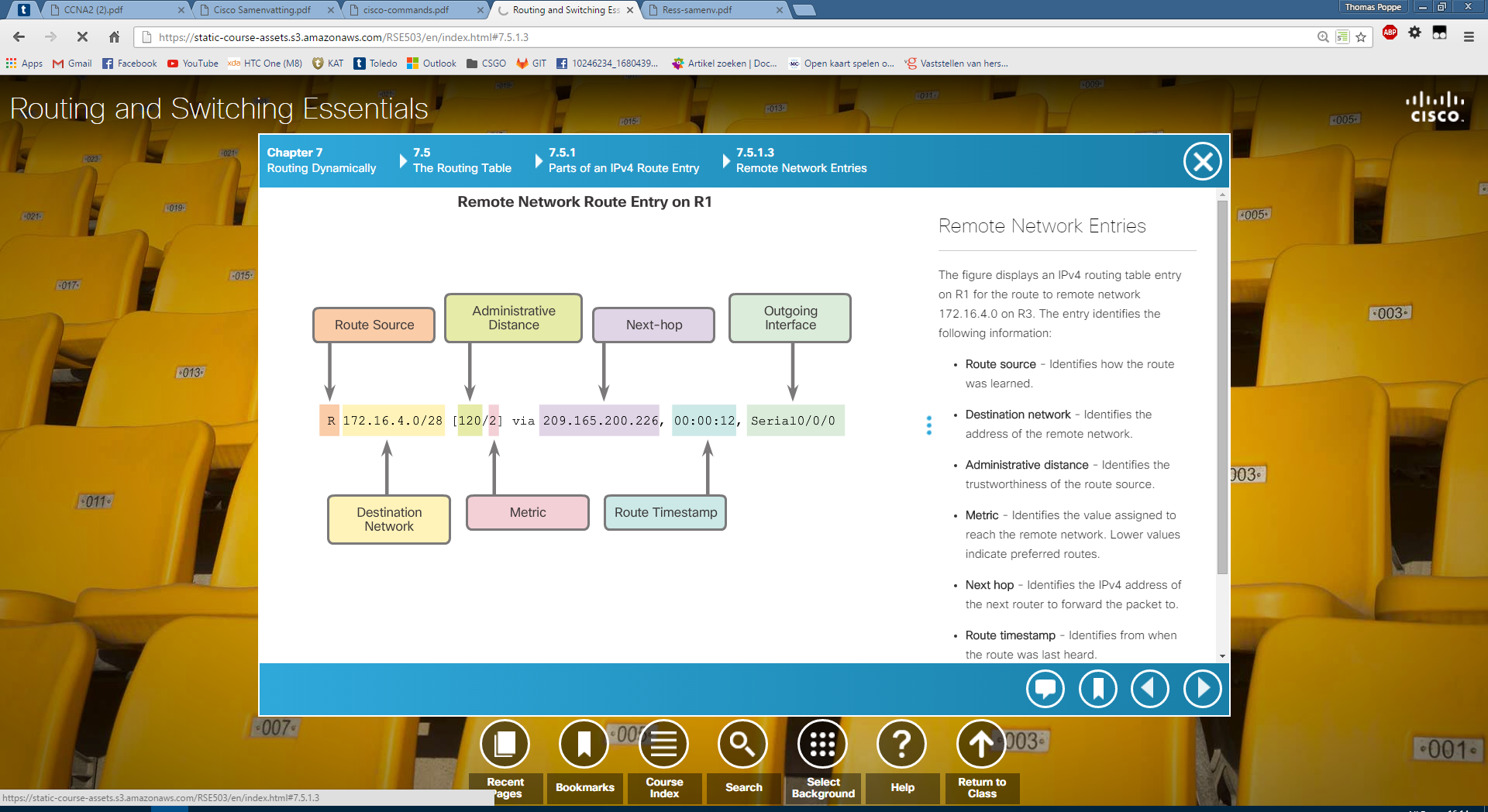
### Why use Link-State Protocols

* **Builds a Topological Map:** Topological Map or SPF tree
* **Fast Convergence:** When receiving LSP, it gets instantly flooded to interface except incoming.
* **Event-driven Updates:** Only send out LSP (only specific change) when a change happens
* **Hierarchical Design:** Link-state routing use the concept of areas

### Disadvantages

* **Memory Requirements:** Additional memory is needed to create LSP & SPF tree.
* **Processing Requirements:** Needs more CPU time to build complete map
* **Bandwidth Requirements:** Flooding Link packets can affect bandwidth (only during start up)

### Remote network example



### Routing Table Terms

* **Ultimate Route:** Next-hop IPv4 address or exit interface. Directly connected, dynamically learned or local routes.
* **Level 1 Route:** Route with subnet mask <= classful mask of network address
  + **Network Route**
  + **Supernet Route**
  + **Default Route**
* **Level 1 Parent Route:** A level 1 route that is subnetted, this can never be an Ultimate.
* **Level 2 Child Route:** Route that is a subnet of a classful network address

# NAT Operation

## NAT Characteristics

### What is a NAT?

* Made to conserve IPv4 addresses
* Allowing private IPv4 in a LAN
* Has one or more public address (NAT Pool)
* Border Router translates internal address to useable external address when a packet is forwarded

### NAT Terminology

* **Inside Address:** Address of device being translated by NAT
* **Outside Address:** Address of the destination device
* **Local Address:** Any address that appears on the inside portion of the network
* **Global Address:** Any address that appears on the outside portion of the network

### Types of NAT

#### Static NAT

* Static IP
* 1 Private <One-To-One Mapping> 1 public

#### Dynamic NAT

* Pool of public addresses
* First-Come, First-served

#### Port Address Translation (PAT)

* Also known as NAT overloading
* # Private <Multiple-To-One Mapping> 1 public
* Each private address is also tracked by a port number for TCP or UDP session
* When a packet is received, the port number is used to do the NAT translation

### Advantages & Disadvantages of a NAT

