**10% 1.0 Network Principles**

1.1 Identify Cisco Express Forwarding concepts

1.1.a FIB

1.1.b Adjacency table

1.2 Explain general network challenges

1.2.a Unicast

* 1 to 1 information sent

1.2.b Out-of-order packets

* Due to load balancing could receive packets out of order
* TCP can sequence the packets or request out of order packets again

1.2.c Asymmetric routing

* Also called unicast flooding
* When a packet goes out 1 L3 Device but comes back on a different one (think HSRP) it might flood it, because it’s not in the ARP table.

1.3 Describe IP operations

1.3.a ICMP Unreachable and Redirects

* Unreachable – Router does not know the route
* Redirect – if next-hop IP address changes the original router can let the host know to use a different path

1.3.b IPv4 and IPv6 fragmentation

1.3.c TTL

* 256 defaults hops prevents routing loops

1.4 Explain TCP operations

1. -> Syn
2. <- Syn + Ack
3. Ack ->

1.4.a IPv4 and IPv6 (P)MTU

1.4.b MSS

* Maxium segment size – that can be sent in a single segment

1.4.c Latency

* Time it takes a packet to get from its source to its destination

1.4.d Windowing

* One or more segments can be sent at a time

1.4.e Bandwidth-delay product

1.4.f Global synchronization

* Also called TCP sync.
* If the router interface fills up the TCP flows can start drop packets

1.5 Describe UDP operations

* Simple with no checks like TCP great for bandwidth utilization

1.5.a Starvation

1.5.b Latency

2013 Cisco Systems, Inc. This document is Cisco Public. Page 2

1.6 Recognize proposed changes to the network

1.6.a Changes to routing protocol parameters

1.6.b Migrate parts of the network to IPv6

1.6.c Routing protocol migration

* Using admin distances, make the new routing protocol higher until you are sure it learned all the routes and is good to go. Then switch it to a lower AD.
* Another way is using route redistribution cutting over the network one section at a time you can move at your own pace and make sure its working

**10% 2.0 Layer 2 Technologies**

2.1 Configure and verify PPP

2.1.a Authentication (PAP, CHAP)

2.1.b PPPoE (client side only)

2.2 Explain Frame Relay

2.2.a Operations

2.2.b Point-to-point

2.2.c Multipoint

**40% 3.0 Layer 3 Technologies**

3.1 Identify, configure, and verify IPv4 addressing and subnetting

3.1.a Address types (Unicast, broadcast, multicast, and VLSM)

3.1.b ARP

3.1.c DHCP relay and server

3.1.d DHCP protocol operations

3.2 Identify IPv6 addressing and subnetting

3.2.a Unicast

3.2.b EUI-64

3.2.c ND, RS/RA

3.2.d Autoconfig (SLAAC)

3.2.e DHCP relay and server

3.2.f DHCP protocol operations

3.3 Configure and verify static routing

3.4 Configure and verify default routing

3.5 Evaluate routing protocol types

3.5.a Distance vector

3.5.b Link state

3.5.c Path vector

3.6 Describe administrative distance

* EIGRP has 3
  + EIGRP via route redistribution have an AD of 170
  + Manual summarization have an AD of 5
    - To see need to do a s hip route for ip and mask
* OSPF has 1 for all of it

3.7 Troubleshoot passive interfaces

3.8 Configure and verify VRF lite

3.9 Configure and verify filtering with any protocol

3.10 Configure and verify redistribution between any routing protocols or routing sources

* Redistribute [protocol/static] subnets
* BE CAREFUL OF SUBOPTIMAL ROUTING AND ROUTING LOOPS

2013 Cisco Systems, Inc. This document is Cisco Public. Page 3

3.11 Configure and verify manual and auto summarization with any routing protocol

Ospf – area # range (or that could all be replaced with “summary-address”) A.B.C.D [wildcard mask]

3.12 Configure and verify policy-based routing

3.13 Identify suboptimal routing

3.14 Explain ROUTE maps

3.15 Configure and verify loop prevention mechanisms

3.15.a Route tagging and filtering

3.15.b Split-horizon

3.15.c Route poisoning

3.16 Configure and verify RIPv2

3.17 Describe RIPng

3.18 Describe EIGRP packet types

* Uses Reliable Transport Protocol (RTP)
* Hello packets handle neighbor discovery and keepalive fore adjacencies. They’re multicast 224.0.0.10
* Acknowledgement packets are hello packets with no data
* Update packets are sent to new neighbors to build routing and topology tables also sent upon a change in the network. Generally, are multicast packets.
  + Uses unicast in replies though
* Query packets are sent when a router loses a successor and has no feasible successor.
* Reply packets are sent in response to query packets, reply packets indicate a new route and use RTP
* TO SEE THESE:
  + Sh ip eigrp traffic

3.19 Configure and verify EIGRP neighbor relationship and authentication

* Router eigrp AS#
* Must be same AS numbers
* Sh ip eigrp neighbors
* sh ip eigrp int detail

AUTHENTICATION

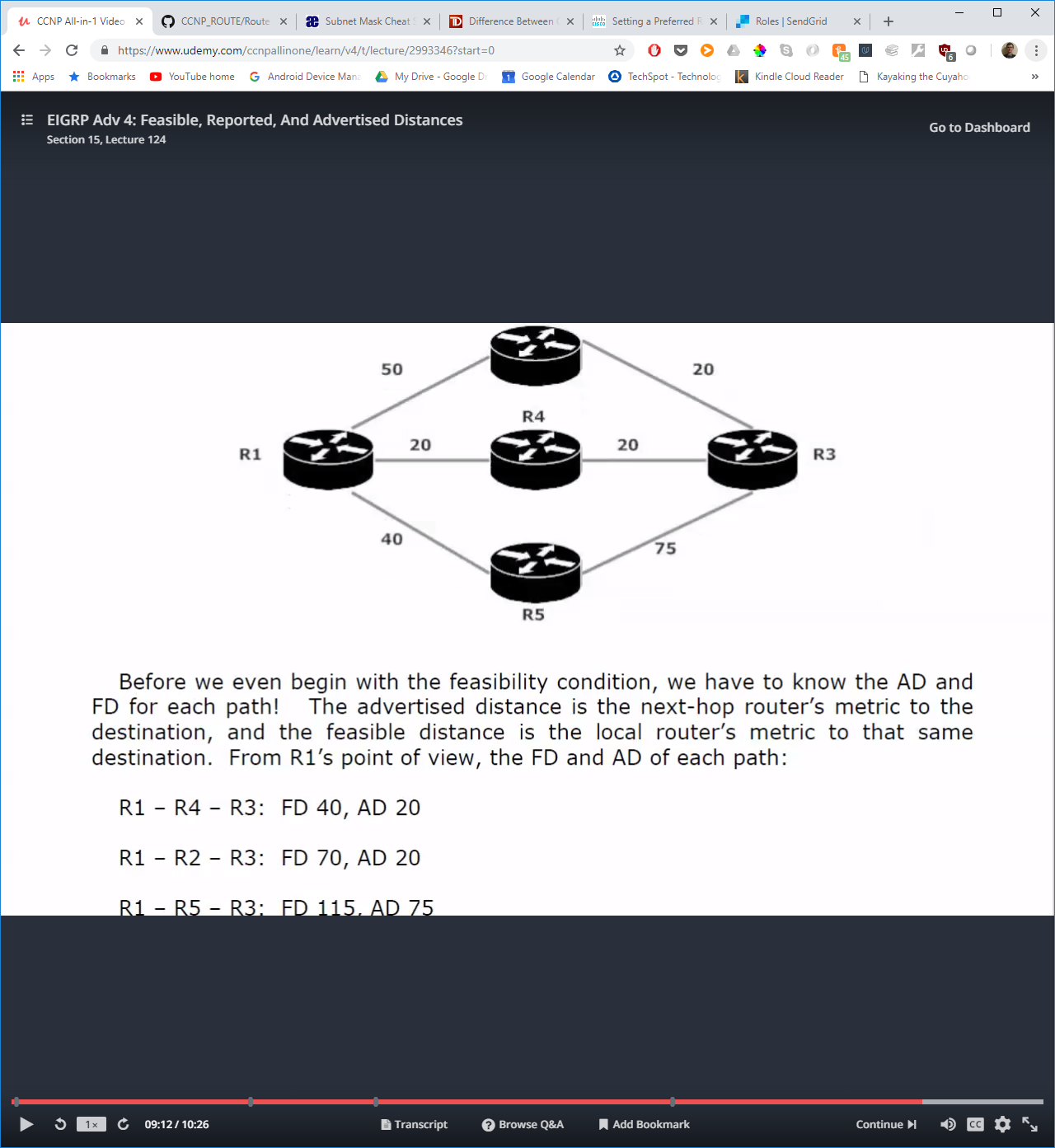
* key chain [name]
  + key [#] <- identifier
  + key-string [password]
* interface [interface]
  + ip authentication mode eigrp [AS] md5
  + ip authentication key-chain eigrp 100 CCNP

3.20 Configure and verify EIGRP stubs

* eigrp stub *command* [ what you want to advertise (connected, static etc…]

3.21 Configure and verify EIGRP load balancing

* Router eigrp AS#
  + Variance #
  + Maxium-paths # (default is 4)
* A Feasible Successor is only so, if its AD is LESS than the FD of the Successor
* The AD is from the Successor Router to the Destination and the FD is that plus the local router to the Succesor metric:



a. Equal cost

b. Unequal cost

3.22 Describe and optimize EIGRP metrics

* K1: Bandwidth
* K2: load
* K3: delay
* K4: reliability
* K5: MTU
* metric weights 0 (Type of service) (This is the K values) 2 0 1 0 0

3.23 Configure and verify EIGRP for IPv6

3.24 Describe OSPF packet types

* Hello
  + Discover, build and maintain ospf neighbor adjacencies
* DBD
  + Database description – to compare databases
* LSR
  + Link state request – inform routers to send the more recent version of missing LSA’s
* LSU
  + Link state update – known as LSA’s
* LSAck – acknowledgement of LSAs

3.25 Configure and verify OSPF neighbor relationship and authentication

* Stuck in 2Way if more than 4 ospf neighbors on a broadcast network
* On the interface for authentication “ip ospf authentication”
  + Then “ip ospf authentication-key WORD”
* On the interface for authentication “ip ospf authentication message-digest”
  + Then – “ip ospf messge-digest 1 md5 WORD”
* “show ip ospf neighbor detail” “show ip ospf interface x/x”
* Change network type with “ip ospf network [network\_type]” example is “point to point”

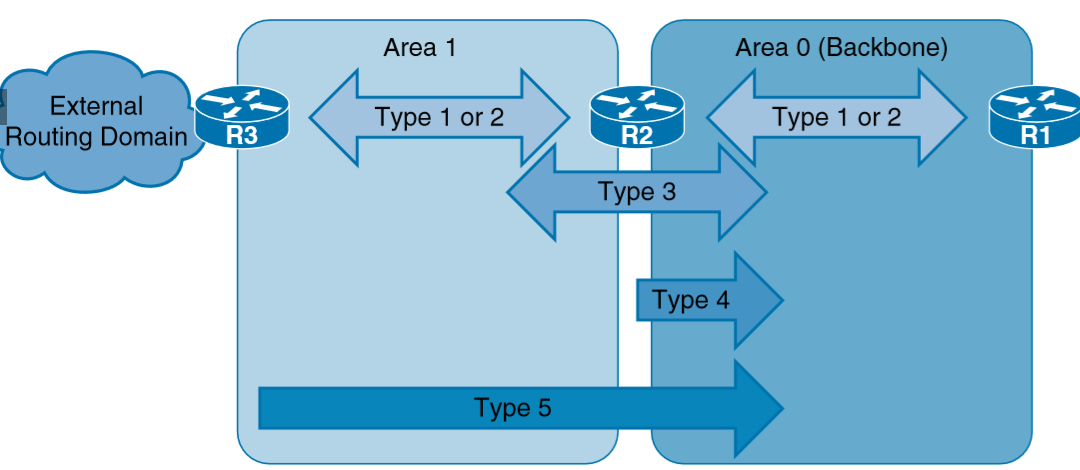
Neighbor OSPF states

1. Down
2. Init
3. Two-Way
4. ExStart
5. Exchange
6. Loading
7. Full

3.26 Configure and verify network types, area types, and router types

a. Point-to-point, multipoint, broadcast, nonbroadcast

b. LSA types

To see on router use “show ip ospf database”

Type 1. Sent by all routers

Type 2. Sent by Drs only for multiaccess networks

Type 3 and 4. Sent by ABRs only – type for summaries of other areas and type 4 for how to reach asbrs

Type 5 and 7. Sent by ASBRs only type 5 external routes and type 7 special external routes for NSSA

Type 6. Reserved for MOSPF (Multicast)

**area type:**

backbone:

Area 0

normal:

Can carry all types of routes

transit:

contains virtual-link

area # virtual-link [router-id]

stub:

* Can contain routes like O and intra area (O IA) but not external ( O E1/E2)
* “area # stub” on both routers

NSSA:

totally stub:

* Can contain only routes to other networks in the total stub area (O) and a single default route for all other routes (O \*IA)
* “area # stub no-summary” on abr and the same on the stub area router without the “no-summary”

c. Internal router:

Area 0 only

backbone router:

At least one interface in area 0

ABR:

All ABR’s are backbone routers, but no vice versa

ASBR (Autonomous system boundary router):

Injecting routes into OSPF domain via route redistribution.

d. Virtual link

* Add a router that is not connected to area 0 via a router that is

3.27 Configure and verify OSPF path preference

* Cost = Reference bandwidth / Interface bandwidth
* Reference bandwidth is set to 100 Mbps by default

3.28 Configure and verify OSPF operations

3.29 Configure and verify OSPF for IPv6

* **ipv6 router ospf** OR (newer) **router ospfv3**
* Need to have at least 1 ipv4 address or router-id command
* Must use ipv6 ospf in interface configuration mode
  + Interface eth0/0
    - Ipv6 ospf 1 area 0

3.30 Describe, configure, and verify BGP peer relationships and authentication

3.30.a Peer group

3.30.b Active, passive

3.30.c States and timers

3.31 Configure and verify eBGP (IPv4 and IPv6 address families)

3.31.a eBGP

3.31.b 4-byte AS number

3.31.c Private AS

3.32 Explain BGP attributes and best-path selection

**10% 4.0 VPN Technologies**

4.1 Configure and verify GRE

4.2 Describe DMVPN (single hub)

4.3 Describe Easy Virtual Networking (EVN)

**10% 5.0 Infrastructure Security**

5.1 Describe IOS AAA using local database

5.2 Describe device security using IOS AAA with TACACS+ and RADIUS

5.2.a AAA with TACACS+ and RADIUS

5.2.b Local privilege authorization fallback

5.3 Configure and verify device access control

5.3.a Lines (VTY, AUX, console)

5.3.b Management plane protection

5.3.c Password encryption

5.4 Configure and verify router security features

5.4.a IPv4 access control lists (standard, extended, time-based)

5.4.b IPv6 traffic filter

5.4.c Unicast reverse path forwarding

**20% 6.0 Infrastructure Services**

6.1 Configure and verify device management

6.1.a Console and VTY

6.1.b Telnet, HTTP, HTTPS, SSH, SCP

6.1.c (T)FTP

6.2 Configure and verify SNMP

6.2.a v2

6.2.b v3

6.3 Configure and verify logging

6.3.a Local logging, syslog, debugs, conditional debugs

6.3.b Timestamps

2013 Cisco Systems, Inc. This document is Cisco Public. Page 5

6.4 Configure and verify Network Time Protocol (NTP)

6.4.a NTP master, client, version 3, version 4

6.4.b NTP authentication

6.5 Configure and verify IPv4 and IPv6 DHCP

6.5.a DHCP client, IOS DHCP server, DHCP relay

6.5.b DHCP options (describe)

6.6 Configure and verify IPv4 Network Address Translation (NAT)

6.6.a Static NAT, dynamic NAT, PAT

6.7 Describe IPv6 NAT

6.7.a NAT64

6.7.b NPTv6

6.8 Describe SLA architecture

6.9 Configure and verify IP SLA

6.9.a ICMP

6.10 Configure and verify tracking objects

6.10.a Tracking objects

6.10.b Tracking different entities (for example, interfaces, IPSLA results)

6.11 Configure and verify Cisco NetFlow

6.11.a NetFlow v5, v9

6.11.b Local retrieval

6.11.c Export (configuration only)