CISSP Domain 4 — Communication and Network Security

Domain 4 — Communication and Network Security

Yes, you need to know the OSI 7-layer model, or at least some of it. This should suffice:

Layer		Device making decisions at this layer
7 6 5	Application Jobs software programs do	ALG, AV, Spam filter, DLP, WAF, etc
4	Transport UDP: Messages to numbered ports TCP: Connections to numbered ports	Firewall
3	Network Relay packets hop by hop to anywhere by IP address: [netidlhostid]	Router
2	Data Link Send frames to HW/MAC addresses	Switch
1	Physical Send and receive 0 vs 1 bits	Repeater (point-to-point link) or hub (star)

Ancient History

This domain contains more ancient history than any other.

Network topologies: Know about **Bus, Tree,** and **Ring** in addition to the modern **Star** and impractical **Mesh.**

Collisions: Shouldn't be an issue with Ethernet switches (unless negotiation failed), but they want you to know about CSMA/CD.

FDDI: It was an attractive campus or metropolitan-area 100 Mbps backbone technology in the early to mid 1990s. Know that it has dual rings, so it can fail to a single ring if a link is cut. It can use copper *or* fiber.

Unexpected Layer 1 details

This wording is subtle, but know it:

- **Concentrators** multiplex connected devices into one signal for transmission.
- **Multiplexors** combine multiple signals into one signal for transmission.

Fiber types:

- Single mode: greater transmission distance
- Multimode: typically up to 400 meters
- POF or Plastic Optical Fiber: significantly shorter range, about 100 meters

Fibre Channel over Ethernet or FCoE: It's a high-speed serial interface using fiber *or* copper.

DSL:

- ADSL or Asymmetric Digital Subscriber Line: downstream transmission rates are much greater than upstream, typically up to 8 Mbps vs 384 kbps.
- VDSL or Very High Bit Rate DSL: much higher rates, maybe 52 Mbps downstream and 2 Mbps upstream, but limited to a much shorter distance from the CO or Central Office to the customer.

Cable modems: Know that they use the DOCSIS protocols.

BPL or **Broadband over Powerline:** This technology hasn't really caught on, due to the severe radio interference problems it causes. But know that it exists.

WiFi range extenders: Know that these exist.

Bluetooth: 802.15. Use Bluetooth 4.x and above, with FIPS approved AES.

Satellite: Useful for remote or sparsely populated areas.

Mobile telephony:

- **CDMA or Code-Division Multiple Access:** Signal is multiplied by a higher-speed bit stream, this is like DS-SS or Direct-Sequence Spread Spectrum.
- **GSM or Global System for Mobiles:** Calls get a channel and a time slot, so both time and frequency multiplexing.
- **Generations:** 1G, 2G, etc., just know that it's evolving, bandwidth is growing, and service is becoming more IP-based.

Unexpected Layer 2 details

Know a little about **MPLS or Multiprotocol Label Switching:** it's a WAN protocol, the first device inserts a label into the frame header, that's used for fast forwarding decisions at all subsequent hops. It lets you do traffic engineering, but it's being replaced by SD-WAN.

You *might* use PPPoE encapsulation on VPNs today.

Unexpected Layer 3 details

Know that the default gateway or default router might be called the **gateway of last resort.**

Ping of Death: This sounds ancient, it was an issue in the 1990s, but it was a Windows vulnerability again in 2013.

Unexpected Layer 4 details

Know that the **Well-Known Ports** are 0-1023.

Unexpected Layer 5 details

PPTP is used to encapsulate and tunnel, as over a VPN. (although its attempt at cryptography is flawed and shouldn't be used)

The modern way to run a VPN is to use **L2TP** to manage the tunnel and **IPsec** to encrypt the traffic.

RPC or Remote Procedure Call protocol: Does what it says.

Unexpected Layer 6 details

Systems use ASCII to represent Unicode. For example, ASCII `&#x0429;` within an HTML file represents Unicode character 0x0429, the Cyrillic letter Щ.

UTF-8 is a character encoding that lets you represent arbitrary Unicode alphabets directly.

Browsers use Unicode internally, and convert other encodings into Unicode. So do search engines.

MP3 or MPEG-1 Audio Layer 3 is a standard audio encoding and compression algorithm. WAVE is another audio encoding standard.

Unexpected Layer 7 details

Know about X11 and the ancient commands `rlogin`, `rcp`, `rsh`, and `ftp`. You should have replaced them some time ago with the SSH versions: `ssh`, `scp`, and `sftp`.

Screen scrapers have been useful to automatically interact with mainframes over TN3270 or similarly old technology.

Application Protocols

DNS: Know that you need A, NS, PTR, and MX records. **More importantly, know about DNSSEC.** I would expect it to be the most common network protocol question topic.

There are DNS resource records for public keys (DNSKEY) and digital signatures (RRSIG). With DNSSEC you have reason to believe that a response is correct, including when the response says that the requested record doesn't exist. My server is in the Google Compute Cloud, and Google's DNS service includes DNSSEC. Notice the RRSIG and DNSKEY records below.

RRSIG records are digital signatures over the indicated preceding record: "RRSIG A" is the signature for the A record, "RRSIG NS" for the set of NS records, and so on.

DNSKEY records are the public signing key, so they're analogous to the CA's digital certificate stored in your browser. You can verify up the chain to the DNS root zone trust anchor. The Cloudflare article is a very nice description.

Cloudflare on DNSSEC

```
$ dig @8.8.8.8 cromwell-intl.com ANY

; <<>> DiG 9.11.3-1ubuntu1.9-Ubuntu <<>> @8.8.8.8 cromwell-intl.com ANY
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23210
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 18, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;cromwell-intl.com.             IN      ANY

;; ANSWER SECTION:
cromwell-intl.com.      3599    IN      A       35.203.182.32
cromwell-intl.com.      3599    IN      RRSIG   A 8 2 3600 20191023184932 20191001184932 1336 cro
cromwell-intl.com.      21599   IN      NS      ns-cloud-c1.googledomains.com.
cromwell-intl.com.      21599   IN      NS      ns-cloud-c2.googledomains.com.
cromwell-intl.com.      21599   IN      NS      ns-cloud-c3.googledomains.com.
cromwell-intl.com.      21599   IN      NS      ns-cloud-c4.googledomains.com.
cromwell-intl.com.      21599   IN      RRSIG   NS 8 2 21600 20191023184932 20191001184932 1336 c
cromwell-intl.com.      21599   IN      SOA     ns-cloud-c1.googledomains.com. cloud-dns-hostmast
cromwell-intl.com.      21599   IN      RRSIG   SOA 8 2 21600 20191023184932 20191001184932 1336
cromwell-intl.com.      299     IN      DNSKEY  256 3 8 AwEAAZhaibf1ewwx+uvJF/LIU0rNbhmtZIVcWnREC
cromwell-intl.com.      299     IN      DNSKEY  257 3 8 AwEAAaJd0s3/TaTnNKSKq4V/DKT00k7oE4s7txW1E
cromwell-intl.com.      299     IN      RRSIG   DNSKEY 8 2 300 20191023184932 20191001184932 1886
cromwell-intl.com.      0       IN      NSEC3PARAM 1 0 1 E3770CCDAA2128C5
cromwell-intl.com.      0       IN      RRSIG   NSEC3PARAM 8 2 0 20191023184932 20191001184932 13
cromwell-intl.com.      299     IN      CDS     18860 8 2 92F4893D8FC1852873EF1C1E2368DFF63A63D8E
cromwell-intl.com.      299     IN      RRSIG   CDS 8 2 300 20191023184932 20191001184932 18860 c
cromwell-intl.com.      3599    IN      CAA     128 issue "letsencrypt.org"
cromwell-intl.com.      3599    IN      RRSIG   CAA 8 2 3600 20191023184932 20191001184932 1336 c

;; Query time: 247 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Oct 04 12:20:50 EDT 2019
;; MSG SIZE  rcvd: 2270
```

SNMP:

- Its verbs are simple, "get" and "set"
- Passwords are called "community strings"
- SNMPv2 had no encryption, community strings were cleartext. SNMPv3 encrypts them.

Active Directory: Microsoft's branding of a combination of 3 protocols using a shared backend database: DNS + LDAP + Kerberos.

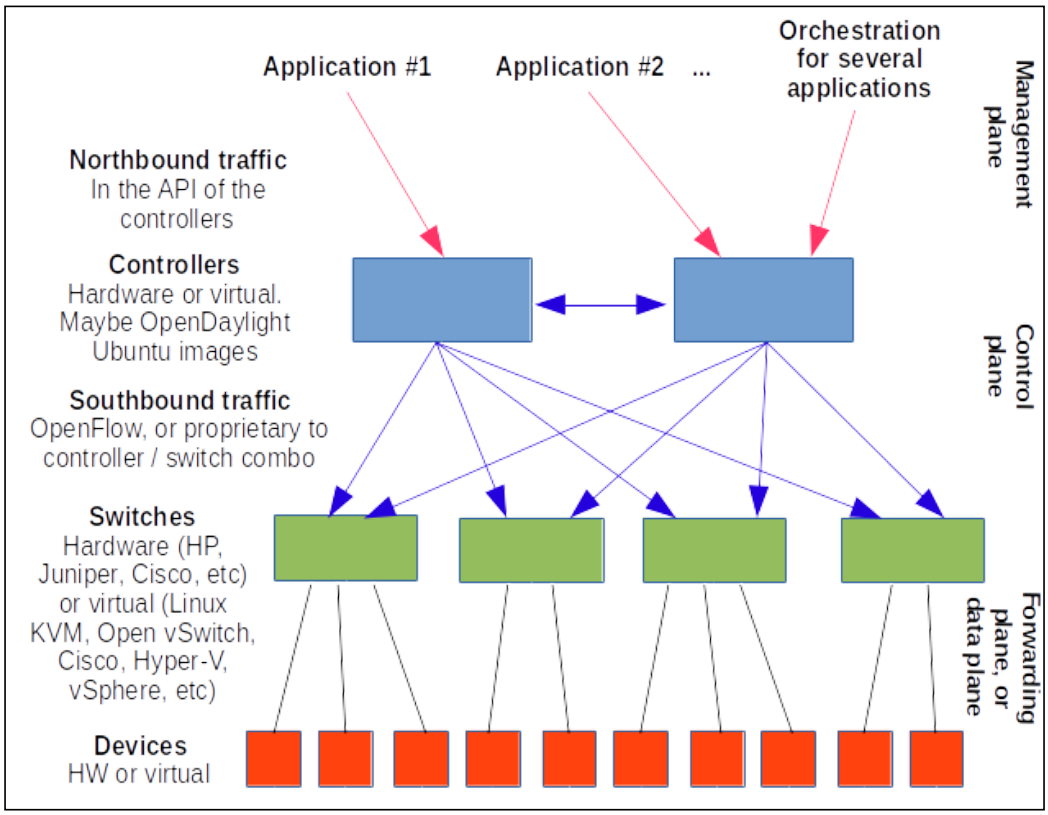
SDN or Software-Defined Networking

Also called NFV or Network Function Virtualization. SD-WAN is replacing MPLS.

Network traffic is split into two classes: **data traffic** flowing from applications to other applications or storage, and **control traffic** flowing from network controller devices to switches and routers altering flows between devices in data centers. This is usually visualized as:

Management or Application Plane
Control Plane
Data Plane

Filling in the details, ignore the non-bold text for the CISSP exam itself:

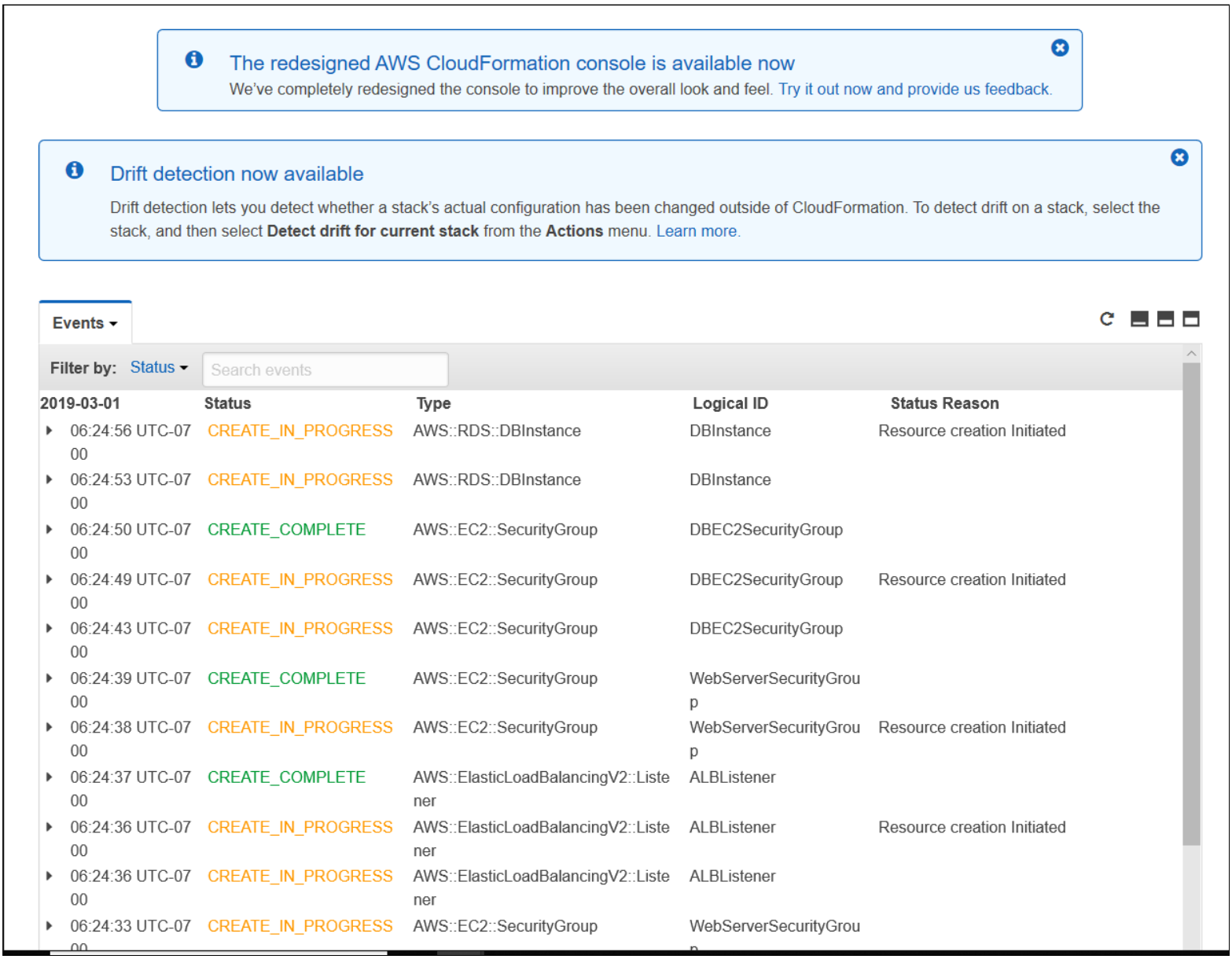


Applications can request traffic flows of desired connectivity and performance. They may do this directly through the API (or Application Programming Interface) of the **controller** through the **northbound traffic.** There may also (or instead) be an**orchestration engine** on the northbound side, which might be considered the *management plane.*

The **controller** sends configuration commands to the **Layer 2-4 switching fabric** through the **southbound traffic.**

The below is *far* deeper than you need to know for the test, but cloud services like Google Cloud and AWS and Microsoft Azure and so on *must* use SDN. Here's what the AWS dashboard shows you of the orchestration parts of a multi-VM deployment with network orchestration. Amazon calls this "CloudFormation". Here we're starting multiple:

- Database instances
- Security groups (firewall rulesets)
- Load balancers



Many thanks to Carter Elmore for the screenshot!

Next-Generation Firewall or NGFW

Similar to UTM or Unified Threat management.

Whitelisting and Blacklisting

Blacklisting is default allow, maintain a growing list of known bad patterns to block.

Whitelisting is default deny, more powerful *if* you can make it work.

Voice over Internet Protocol or VoIP

Uses Session Initiation Protocol or SIP, so any SIP-capable device can talk to any other. SIP manages multimedia connections, including the codec selection.

Privacy extensions to SIP include encryption and caller ID suppression.

Internet Relay Chat or IRC

Unencrypted, and user identification is easy spoofed.

SOme IRC clients can execute scripts. This was intended to simplify administration, but as they're executed with the user's privileges with little to no protection, they're an attractive target for social engineering.

SPIM is Spam over instant messaging.

IPsec

Know: AH, ESP, SA or Security Association, Transport Mode, Tunnel Mode, and IKE or Internet Key Exchange.