ELT-53106 computer networking 2 **(11.05.2016)**

Instructor: Alexander Pyattaev

Calculators are NOT allowed

Answers MUST be given on the question sheet

Question sheet MUST be returned

Student name:

Student number:

PAY ATTENTION to the exam rules.

Not reading them may harm your final score.

- **Exam structure:**
  - The exam lasts 3 hours. The questions are split into 3 sections, each with its own kind of questions. Guideline times are 45, 45 and 90 minutes for each section respectively. If you fall behind, proceed to the next section, and then return to questions you skipped if time allows.
  - The maximum number of points you can get from this exam is 100. 50 points are necessary to pass.
- Mark your answers on the sheets given to you - do not submit any other papers. You may use the free space of the exam papers as scratch paper. Scratches and drafts are not checked.
- Read questions very carefully before answering.
  - If you find any issues in the exam questions (typos, formulation problems etc), please indicate them for possible bonus points. If you believe you have to make additional assumptions to give an answer, do so, and write them down next to question text. The additional assumptions you make do not affect the score as long as they result in correct answers.
- **For multiple choice questions:**
  - `circle` **all the correct options.** Please, do not tick, underline, strike out or otherwise indicate any of the options. Remember that any number of options may need to be circled;
  - there is always at least one correct option to be marked;
  - if and only if **all** correct options are marked, the announced number of points is added to the exam score. Each incorrectly marked option, as well as unmarked correct option, removes 2 points from the question score. The question score does not go below zero.
- **For other questions:**
  - **give the answer in the space provided.** If it is insufficient, you are probably doing something wrong. In addition, one picture is often worth more than a 1000 words, so don't hesitate to draw one;
  - open questions are rated based on teacher's decisions, unless otherwise indicated in the question text.
- Please remember to provide feedback in Kaiku (even if you provide feedback in the exam paper)
- I have read and understood the rules and regulations [Tick here].

Remember! Most of the exam questions may be answered with deduction without preparation.

It is not about what you have memorized, but about how you think.

Exam questions

A Multiple choice (30 points)

A.1 Routing and forwarding [3 points]

Which of the following statements are true in context of routing and forwarding?

1. Routing algorithms find paths to all destinations through the network
2. Forwarding is the procedure choosing a next hop to send a packet towards its ultimate destination
3. To forward a packet correctly, a router must know the topology of the entire network
4. The routing protocols are application-layer programs, whose main purpose is convenience of configuration for large networks.

A.2 Distance-vector routing protocols [3 points]

Which of the following statements are true for distance-vector (DV) routing (e.g. RIP, AODV)?

1. DV protocols do not typically learn the entire topology of the network, instead relying on the updates shared between immediate neighbors
2. The cost of a route is **always** cumulative cost of all links in it
3. DV protocols can have issues removing routes when they become unavailable
4. Routers running RIP periodically send their entire routing tables to their neighbors

A.3 Link-state routing protocols [3 points]

Which of the following statements are true for link-state (LS) protocols (e.g. OSPF)?

1. The cost of a route is **always** cumulative cost of all links in it
2. Every router **must** to know the topology of the **entire** domain under LS protocol's control to calculate routes
3. OSPF protocol allows for two (and exactly two) levels of hierarchy within its domain.
4. A special flooding procedure is often necessary to enable routers to learn the network topology

A.4 Inter-AS routing, BGP protocol [3 points]

Which of the following statements are true for BGP(inter-AS routing in general)?

1. BGP is used to advertise the subnets that are present inside an AS.
2. BGP packets are carried over TCP, and thus require route to each peer to be configured otherwise
3. BGP is commonly run only on the AS border router, especially if it is the only gateway to Internet
4. If multiple gateways lead to an AS, (interior-)BGP should run also on the routers inside the AS

A.5 Label switching [3 points]

Which of the following statements apply to the label switching (LS) procedure?

1. In LS networks forwarding decisions are based on labels, rather than IPs and netmasks.
2. LS protocols may require IP routing support on all hops for initial configuration of labels and fallback
3. LS forwarding complexity scales with the number of the border routers in LS domain, and does not depend on the number of subnets in the Internet
4. LS forwarding procedure is typically less resource intensive than conventional IP forwarding

A.6 IPv6 protocol [3 points]

Which of the following statements apply to the IPv6 protocol?

1. IPv6 follows the same forwarding procedure as IPv4, except for address length
2. It is common for IPv6 hosts to have multiple addresses on the same interface
3. IPv6 does not allocate a specially reserved broadcast and/or router address in each subnet
4. IPv6 spec includes common IPv4 service protocols (e.g. ARP, DHCP, and some others) as part of ICMPv6

A.7 IPv6 transition [3 points]

Please indicate what kind of backwards compatibility solutions are possible between IPv4 and IPv6

1. Every IPv4 address is mapped into a valid IPv6 address, facilitating concurrent usage
2. IPv6 addressing scheme discourages the use of NATs (although does not prohibit it)
3. A host can run both versions of IP at the same time using different IP addresses
4. One can tunnel IPv6 packets inside IPv4 packets

A.8 Virtual Private Networks [3 points]

Which of the following apply to secure VPN

1. VPN allows one to logically join two networks which do not have an L2 link between them
2. VPN protocols do not always provide encryption of the data between endpoints
3. VPN could be established as a L3, L4 or L7 protocol, depending on use-case
4. VPN is a very good solution to improve security of a home network

A.9 IPSec [3 points]

Indicate which of the following are true

1. IPsec is a framework that allows to build encrypted VPN tunnels in IP
2. IPsec can be used to provide security without tunneling (VPN function)
3. IPSec uses RSA encryption algorithm for transport
4. IPSec supports auto-configuration, and is a good solution for remote-access VPN

A.10 Mobile IPv6 [3 points]

Reminder: correspondent node is a node in the Internet (e.g. google.com) that mobile node is communicating with. Home agent is the router in the home network. Which statements are true for MIPv6?

1. MIPv6 is the mobility solution of choice in (GSM/3G/LTE) cellular networks
2. MIPv6 by default uses relayed delivery when mobile node is not in home network, where all packets are tunneled via the home agent
3. MIPv6 allows routing packets directly from correspondent node to the actual address of the mobile node after changing the access point, while preserving connections
4. MIPv6 allows a device in the home network to continue communication with mobile node that leaves home network

B Short open questions (30 points)

B.1 Route redistribution [6 points]

Consider you are maintaining a small office network. The office has 2 branches, one of them is small (130.230.0.0/24), the second one is larger (130.230.32.0/20), both use the OSPF protocol for interior routing. In addition, each branch has a link to the Internet from their respective gateways (**A** and **B**), but links are provided by different ISP's (ISP_A and ISP_B). There is one link (C_A<->C_B) between branches, *and it should never be used for traffic that goes towards Internet. BGP must be used when communicating with both ISP's.*

Which of the subnets will be advertised as reachable for each of the ISP's?
ISP A:
ISP B:

What should happen on link C_A<->C_B?

B.2 Secure connection setup procedures [6 points]

Put the operations: *A:Client Authentication (login&password check), B:Transport encryption key negotiation, C:Transport layer connection setup, D:Server Identity Verification* in the order they are applied when **setting up a secure connection** (e.g. in SSH/TLS/SSL). Correct order yields full points, incorrect - zero.

Order	Operation	Motivation (not compulsory)
1		
2		
3		
4		

B.3 Distributing encryption keys [6 points]

Nearly all modern encryption algorithms are based on public key cryptography. The PK crypto systems assume that every node initiating a connection has a copy of its peer's public key, which was obtained over a reliable (but not secret) channel. In practice, this means that "someone" (Trusted Authority) is responsible for holding all sorts of public keys for various hosts. Indicate at least one alternative approach to solve this problem and avoid having a single Trusted Authority.

Answer:

B.4 Protocol stack [6 points]

Assume that there is an IPv4 IPSec tunnel (in authenticated header tunnel mode) running through the network. An observer is capturing the packets with Wireshark**.** A single HTTPS packet with payload data is intercepted. Which protocols would be able to identify? Assume that Ethernet is the data-link layer, and no extra features are used (such as VLAN, MPLS, IP options etc).

Please draw a small picture illustrating the view of the observer, add text as necessary:

B.5 Traffic shaping [6 points]

Random early detection (RED) is an advanced traffic shaping function that begins to drop random TCP packets when it detects that the incoming queue of the router is almost full (e.g. 80% full). Explain briefly on which routers should the RED be deployed in a typical network.

Answer:

C Short exercises (40 points)

C.1 QoS assurance [10 points]

Your boss asked you to upgrade WiFi network in TUT. It is known, that the staff often uses Skype to make calls to their colleagues, and there are issues with the connection quality, such as packet loss, and excessive lag in the voice when using WiFi. The problem does not happen when Ethernet is used.

However, you observe that the WiFi installation itself is an extremely well-designed Cisco installation, with maximal loads on the WiFi link **always** below 50% of capacity. Naturally, you need to collect more data, where would you look for the problem? Speculate would could be the likely source of the problem and the solution?

Answer:

C.2 Protection of the service from attacks [10 points]

A Panama-based legal company has decided to improve its security practices. They believe, that the remote-access system they use for their employee's laptops is not sufficiently secure. In particular, they use a PPtP-based remote-access VPN, where a 2048 bit RSA keys are used to authenticate both the VPN server and the connecting client. The keys stored on the client machine are encrypted with a password. 512bit symmetric key is used to encrypt the actual packets. Once inside the VPN, an employee may access the internal web pages and the database where confidential data is stored by supplying a username and password.

With such overkill encryption in the VPN, why would they be concerned about remote-access security? Illustrate on a picture an attack that you would try to execute on such a system.

Answer [draw a picture to illustrate if appropriate]:

C.3 Multicast [10 points]

Consider you are hired by Blizzard to improve the performance of their latest release of World of Warcraft(WoW) massively multiplayer online game (MMOG). The game world is partitioned into several relatively small segments, where at most 500 players are present at any given moment. Each segment is handled by its own dedicated server, but players from across several continents may wish to play in the same segment. The server acts as a relay for **all** data related to the gaming process, i.e no packets are ever sent from user to user. There are, obviously, issues with network quality.

- The movements of other players often appear jumpy and not smooth;
- Significant portion of server resources is consumed forwarding position updates;
- Whenever a new player walks into a particular segment, the server has to spend lots of time sending the description of his avatar to all players already there.

On the CN2 course you have heard that multicast may address some or all of the above issues. How would you make it happen?

Answer [draw picture if necessary]:

C.4 Massive streaming storage question [10 points]

In a very secret underground facility in Dusseldorf, VW engineers are still fixing bugs in their Diesel engines. In the new engine, everything (including individual bearings!) is digitally monitored lots of data is collected during the tests. An engine has at most 1000 sensors, each producing 32 bit samples at 1 megasample/second. The samples are collected by a specialized control unit and must be stored for further analysis.

Your task is to design a system that would store all of the data produced during the tests. The system must enable reliable and scalable (e.g. it should be possible to add more storage). The basic storage unit in your possession is a 1 TB hard drive, with sustained write speed of 10 Mbytes/s. Exact calculations are not required, general dimensioning and architecture are critical.

Answer:

Thank you for taking Computer Networking 2 course! Provide course quality feedback in Kaiku!

Free-form feedback on the exam questions quality (this section does not affect the grades):

Hope to see you next year on our courses on Network Analysis and Dimensioning.