Microsoft

CompTIA® Security+™

Exam SY0-301

Rapid Review

CompTIA AUTHORIZED PARTNER

CompTIA APPROVED QUALITY CONTENT

Michael Gregg

Rapid Review

CompTIA Security+ Exam SY0-301

Assess your readiness for the CompTIA Security+ Exam SY0-301—and quickly identify where you need to focus and practice. This practical, streamlined guide walks you through each exam objective, providing "need to know" checklists, review questions, tips, and links to further study—all designed to help bolster your preparation.

Reinforce your exam prep with a *Rapid Review* of these objectives:

- Network security
- Compliance and operational security
- Threats and vulnerabilities
- Application, data, and host security
- Access control and identity management
- Cryptography

This book is an ideal complement to the in-depth training of the Microsoft Press® *Training Kit* and other exam-prep resources for CompTIA Security+ Exam SY0-301.

ISBN: 978-0-7356-6685-6

U.S.A. $29.99
Canada $31.99
[*Recommended*]

Certification/ CompTIA Security+

CompTIA Security+

ABOUT THE AUTHOR

Michael Gregg is founder and president of an IT security consulting firm. He is Security+, A+, Network+, CISSP, SSCP, CISA, MCSE, MCT, CTT+, CNA, CCNA, CIW Security Analyst, CCE, CEH, CHFI, DCNP, and ES Dragon IDS certified.

CompTIA AUTHORIZED PARTNER

CompTIA APPROVED QUALITY CONTENT

Microsoft®

Microsoft

CompTIA® Security+™ Rapid Review (Exam SY0-301)

Michael Gregg

ISBN: 978-0-735-66685-6

1 2 3 4 5 6 7 8 9 LSI 7 6 5 4 3 2

Printed and bound in the United States of America.

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at *mspinput@microsoft.com*. Please tell us what you think of this book at *http://www.microsoft.com/learning/booksurvey*.

Acquisitions and Developmental Editor: Kenyon Brown
Production Editor: Kristen Borg
Editorial Production: Octal Publishing, Inc.
Technical Reviewer: Randy Muller
Copyeditor: Bob Russell, Octal Publishing, Inc.
Indexer: Bob Pfahler
Cover Design: Best & Company Design
Cover Composition: Karen Montgomery
Illustrator: Rebecca Demarest

Contents at a Glance

Contents

Introduction

This Rapid Review is intended to assist you as you study for the CompTIA Security+ exam SY0-301. The Rapid Review series is designed for exam candidates who already have a good grasp of the exam objectives through a combination of experience, skills, and study, but who would also like a concise review guide to help them assess their readiness for the exam.

The SY0-301 exam is aimed at an IT security professional who has the following attributes:

- A minimum of two years of experience in IT administration with a focus on security
- Day-to-day *technical* information security experience
- Broad knowledge of security concerns and implementation

Although this experience would preferably include foundation-level security skills and knowledge, you might have real-world experience. Most candidates who take this exam have the knowledge and skills required to identify risk and participate in risk mitigation activities; provide infrastructure, application, operational and information security; apply security controls to maintain confidentiality, integrity and availability; identify appropriate technologies and products; and operate with an awareness of applicable policies, laws and regulations. It is important to note that you should have some real-world experience with security prior to taking the SY0-301 exam, and that having practical knowledge is a key component to achieving a passing mark.

This book will review every concept described in the following exam objective domains:

- 1.0 Network Security
- 2.0 Compliance and Operational Security
- 3.0 Threats and Vulnerabilities
- 4.0 Application, Data and Host Security
- 5.0 Access Control and Identity Management
- 6.0 Cryptography

This is a Rapid Review and not a comprehensive guide like the *CompTIA Security+ Training Kit*. The book covers every exam objective on the SY0-301 exam, but it will not necessarily cover every exam question. CompTIA regularly adds new questions to the exam, making it impossible for this (or any) book to provide every answer. Instead, this book is meant to supplement your existing independent study and real-world experience with the product.

If you encounter a topic in this book with which you do not feel completely comfortable, you can visit the links described in the text, research the topic further by using other websites, and consult support forums. If you review a topic and find that you don't understand it, you should consider consulting the *CompTIA Security+ Training Kit* from Microsoft Press. You can also purchase practice exams or use the one available with the Training Kit to further determine if you have need further study on particular topics.

NOTE **The Rapid Review is designed to assess your readiness for the SY0-301 exam. It is not designed as a comprehensive exam preparation guide. If you need that level of training for any or all of the exam objectives covered in this book, we suggest the *CompTIA Security+ Training Kit* (ISBN: 9780735664265). The Training Kit provides comprehensive coverage of each SY0-301 exam objective, along with exercises, review questions, and practice tests. The Training Kit also includes a discount voucher for the exam.**

CompTIA Professional Certification Program

CompTIA professional certifications cover the technical skills and knowledge needed to succeed in a specific IT career. Certification is a vendor-neutral credential. An exam is an internationally recognized validation of skills and knowledge that is used by organizations and professionals around the globe. CompTIA certification is ISO 17024 Accredited (Personnel Certification Accreditation) and, as such, undergoes regular reviews and updates to the exam objectives. CompTIA exam objectives reflect the subject areas in an edition of an exam and result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an professional with a number of years of experience.

MORE INFO **For a full list of CompTIA certifications, go to *http://certification.comptia.org/getCertified/certifications.aspx*.**

Acknowledgments

I would like to thank my wife, Christine, for all her support. I would also like to thank all of the individuals at O'Reilly Media for their help in making this book a reality.

Support & Feedback

The following sections provide information on errata, book support, feedback, and contact information.

Errata

We've made every effort to ensure the accuracy of this book and its companion content. Any errors that have been reported since this book was published are listed on our Microsoft Press site:

http://www.microsoftpressstore.com/title/9780735666856

If you find an error that is not already listed, you can report it to us through the same page.

If you need additional support, email Microsoft Press Book Support at *mspinput@microsoft.com*.

Please note that product support for Microsoft software is not offered through the addresses above.

We Want to Hear from You

At Microsoft Press, your satisfaction is our top priority, and your feedback our most valuable asset. Please tell us what you think of this book at:

http://www.microsoft.com/learning/booksurvey

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in Touch

Let's keep the conversation going! We're on Twitter: *http://twitter.com/MicrosoftPress*

Preparing for the Exam

CompTIA certification exams are a great way to build your résumé and let the world know about your level of expertise. Certification exams validate your real-world job experience and product knowledge. Although there is no substitute for on-the-job experience, preparation through study and hands-on practice can help you to prepare for the exam. We recommend that you augment your exam preparation plan by using a combination of available study materials and courses. For example, you might use the Rapid Review and another training kit for your "at home" preparation, and take a CompTIA professional certification course for the classroom experience. Choose the combination that you think works best for you.

CHAPTER 1

Network Security

Roughly 21 percent of the SY0-301 exam comes from this domain. You need to have a good grasp of implementing, distinguishing, and applying proper network security techniques. You need to know how to explain the function and purpose of basic network devices. Additionally, you need to know how to apply basic network security principles and how to distinguish network design elements, such as demilitarized zones (DMZs), remote access, cloud computing, and network access control (NAC). You also need to understand common protocols and their port numbers. Finally, you need to understand how to implement wireless systems in a secure manner. This chapter covers the following objectives:

This chapter covers the following objectives:

- Objective 1.1: Explain the security function and purpose of network devices and technologies.
- Objective 1.2: Apply and implement secure network administration principles.
- Objective 1.3: Distinguish and differentiate network design elements and compounds.
- Objective 1.4: Implement and use common protocols.
- Objective 1.5: Identify commonly used default network ports.
- Objective 1.6: Implement wireless network in a secure manner.

Objective 1.1: Explain the security function and purpose of network devices and technologies

In this exam Objective, you might be tested on the security function and purpose of network devices and technologies. You might be asked about firewalls, routers, switches, intrusion detection systems (IDS), sniffers, and many other web firewalls and URL filtering devices.

Exam need to know...

- Specify the purpose and function of a firewall

  For example: Do you know that firewalls typically reside at the edge of the network between the Internet and the trusted internal network?

- Specify the security function and purpose of routers

  For example: Do you know that routers reside at Layer 3 of the Open Systems Interconnection (OSI) model and that they can be used as a basic packet filter?
- Specify the security function and purpose of a switch

  For example: Do you know that switches physically segment network traffic, make it harder for attackers to sniff traffic, and can be used to set up virtual LANs (VLANs)?
- Specify the security function and purpose of a load balancer

  For example: Do you know that a load balancer is used to distribute the workload among multiple computers or a cluster of computers?
- Specify the function and purpose of a proxy

  For example: Do you know that a proxy server acts as an intermediary that processes requests from clients seeking resources from other servers?
- Specify the function and purpose of a web security gateway

  For example: Do you know that a web security gateway filters unwanted traffic and malware from endpoint web/Internet traffic and enforces ingress and egress rules?
- Know the function and purpose of Virtual Private Network concentrators

  For example: Do you know that VPN concentrators are designed to handle a very large number of VPN tunnels?
- Know the function and purpose of a network intrusion detection system and a host intrusion detection system

  For example: Do you know what tool is used at the edge of the network to detect anomalies or unusual traffic?
- Explain protocol analyzers

  For example: Can you explain what hardware or software tool can be used to examine network traffic?
- Understand the purpose and function of sniffers

  For example: Do you know what tool can be used to capture clear text user names and passwords from a network connection?
- Know the purpose and security function of SPAM filters and all-in-one security devices

  For example: Do you know which tool can be used to block fake emails and messages from unknown recipients?
- Understand the purpose and function of web application firewalls and how they are different from network firewalls

  For example: Can you describe what type of tool can be used to protect web applications and filter malicious traffic such as SQL injection attacks?
- Define URL filtering, content inspection, and malware inspection

  For example: Do you know what type of service is needed to check the origin or content of a webpage against a set of rules as provided by a company or person?

Firewalls

Firewalls play a key role in network security because they reside at the edge of the network and act as a first line of defense. Firewalls are designed to inspect incoming and outgoing network traffic. Firewall rules can be configured to allow or block certain types of traffic.

True or false? Firewalls can use different types of screening techniques. As an example, a firewall can filter traffic based on a source or destination IP address.

Answer: *True.* Firewalls can filter traffic by many different criteria. This can include source or destination IP address, URL, traffic content, TCP or UDP settings, and so on.

> ***EXAM TIP*** **Because firewalls play such a key role in network security, you can expect to see questions on the exam that ask you about their functions and how they are used.**

True or false? A firewall can be embedded or part of a router.

Answer: *True.* Routers have the ability to act as basic firewalls.

> ***MORE INFO*** **To learn more about firewalls, consult the TechNet document at *http://technet.microsoft.com/en-us/library/cc700820.aspx*.**

Routers

Routers operate at Layer 3 of the OSI model, and as such, they deal with logical addresses. A commonly used logical addressing scheme is Internet Protocol (IP). Routers enhance networks by segmenting physical traffic. Routers also can be used to connect different network types and to span a distance. Routers provide a valuable security function because they can connect different networks and simultaneously provide some filtering of network traffic. This might be two or more LANs or WANs. Routers are considered edge devices because they are located where two or more networks connect.

True or false? By default, routers pass Layer 2, physical traffic.

Answer: *False.* Routers do not pass Layer 2 traffic. Routers deal with Layer 3 traffic.

True or false? A router can be used as a basic security device.

Answer: *True.* Routers have built-in functionality that can filter traffic. Routers also block physical traffic, so they can be used to separate departments; for example, You could set up a router so that accounting cannot see marketing network traffic.

True or false? Routers are only installed at the edge of corporate networks.

Answer: *False.* Although routers can be installed at the edge of a network, such as between a corporate network and the Internet, they can also be used to separate LANs.

> ***MORE INFO*** **To learn more about routers, consult the TechNet document at *http://technet.microsoft.com/en-us/network/bb545655*.**

Switches

Switches are one of the key components of most modern networks. Switches replaced *hubs*; they are a more intelligent piece of hardware. You can use switches to connect multiple computers and other network devices to one another. Switches segment traffic; for example, users on port A and port B can have a conversation while users on port C and port D carry on a separate conversation. Switches make it more difficult for an attacker to sniff traffic because the traffic is forwarded only to an appropriate connected device.

True or false? Switches offer better performance than a hub.

Answer: *True.* A switch is capable of inspecting traffic as it is received and then forwarding it only to the specified destination device. By delivering traffic only to the specified device, switches conserve network bandwidth.

True or false? Unlike hubs, switches make it easier for an attacker to intercept and sniff network traffic.

Answer: *False.* Switches make it more difficult to carry out an attack. Hubs send all traffic to all destination devices, whereas switches send traffic only to a specified device.

Load balancers

A load balancer is used to distribute many different types of traffic across a group or cluster of computers. Load balancers can be software or hardware. Load balancing serves a security function because it hides the addresses of the devices behind the load balancer.

True or false? One of the advantages of a load balancer is that it can distribute traffic to a busy website among many different web servers.

Answer: *True.* Load balancers are used to even out web traffic to busy sites. An organization might have many web servers; the load balancer distributes this load among many individual computers.

True or false? A load balancer can be used to hide internal IP addresses.

Answer: *True.* Load balancers can be used to hide the internal IP address of individual devices.

Proxies

A proxy is an entity that exists between two other entities and acts on behalf of one of those entities. The purpose of a proxy as it relates to networks is to act as a buffer between a user and a web server. Proxy servers can also be used to cache content.

True or false? Proxy servers request content on behalf of the client.

Answer: *True.* A proxy server provides web resources by connecting to a web server and requesting the service on behalf of the client.

True or false? Proxy servers offer no speed advantages.

Answer: *False.* Proxy servers can speed up access to resources by using caching.

Web security gateways

Web security gateways are designed to filter malicious traffic and to add a layer of protection for the web server.

True or false? Web security gateways offer secure communication between the client and the server.

Answer: *False.* Web server gateways do not protect web applications. This would be the role of Secure Sockets Layer (SSL) or application firewalls.

True or false? A web security gateway cannot be used to prevent end users from downloading known malware from the Internet.

Answer: *False.* A web security gateway filters unwanted software or malware from endpoint web/Internet traffic and enforces corporate and regulatory policy compliance.

> ***EXAM TIP*** **Web server gateways are just one component of Internet security. An in-depth defense requires IDS, encryption, web application firewalls, and so on.**

VPN concentrators

Virtual Private Network (VPN) concentrators are used to manage large numbers of VPN connections. VPNs are critical because they provide a secure means of communication across open networks so that remote users can communicate with a company securely. VPN concentrators are ideal when you require a single device to handle a large number of incoming VPN tunnels.

True or false? One common type of VPN concentrator uses Internet Protocol Security (IPsec).

Answer: *True.* Two common types of VPN concentrators include IPsec and SSL.

NIDS and NIPS (Behavior based, signature based, anomaly based, heuristic)

Intrusion detection plays a key role in monitoring for and detecting malicious activity. There are two main types of intrusion detection: network intrusion detection system (NIDS), and host intrusion detection system (HIDS). Network-based intrusion detection uses a network-based sensor (or sensors) that is connected to a switch or hub port to collect network traffic. Host-based intrusion detection consists of an agent on a host that analyzes system activity.

True or false? NIDS are effective for preventing attacks.

Answer: *False.* NIDS can detect attacks and set off an alarm, but they do not prevent an attack from occurring.

True or false? HIDS are effective at detecting malicious network traffic as it enters the network.

Answer: *False.* HIDS are installed on individual computers. They are not network-based devices; that is the role of NIDS.

Protocol Analyzers

Protocol analyzers are network or software devices that capture and analyze network traffic.

> ***EXAM TIP*** **Although protocol analyzers are not intended to be malicious tools, you should be aware that they can be used to capture clear-text information.**

True or false? By default, protocol analyzers can be used to see all traffic on a switched network.

Answer: *False.* Protocol analyzers work best when used on a hub. If used on a switch, the protocol analyzer will only see the traffic on the specific port into which the analyzer is plugged. Higher-end switches can be configured to share traffic by means of *spanning*, but they must be configured to do so.

True or false? Protocol analyzers can be used to troubleshoot network problems.

Answer: *True.* Protocol analyzers are designed for network troubleshooting. Protocol analyzers vary in their capabilities, but most of them are able to display data in multiple views, automatically detect errors, and help the user to determine the cause of errors.

> ***MORE INFO*** **To learn more about protocol analyzers, consult the TechNet document at *http://blogs.technet.com/b/netmon/*.**

Sniffers

Sniffers are another name for a protocol analyzer. Generally, they describe a software product designed to capture and analyze network traffic. Sniffers work by placing the NIC into promiscuous mode so that the sniffer can detect all the traffic that is present. Depending on how the sniffer is configured, it can capture all network traffic or just the traffic from a single device within the network. When used with a switch, the sniffer must be specially configured to gain access to all traffic from other systems on the network.

True or false? Although sniffers are valuable troubleshooting tools, they can be used maliciously.

Answer: *True.* Sniffers can be used to capture traffic that is not encrypted. An attacker might be able to intercept and capture clear-text user names and passwords.

> ***MORE INFO*** **To learn more about Microsoft's Network Monitor sniffer program, review the download at *http://www.microsoft.com/download/en/details.aspx?id=4865*.**

Spam filter, all-in-one security appliances

Blocking malicious traffic and filtering out bogus email is an important job for most security professionals. Surveys show that a large amount of email is spam. Spam filters are designed to filter out these unwanted emails before they reach the end user.

One way to do this is by using all-in-one security devices. These devices combine not just spam filtering, but they can also act as a firewall and a malware detection unit. The advantage of these multipurpose security devices is that they consolidate all the functions of a firewall, such as spam filtering, intrusion prevention, and more. An all-in-one device can be easy to manage, but you must also consider that it can be a single point of failure.

True or false? Although it might be annoying, spam is typically never malicious.

Answer: *False.* Spam can be nothing more than ads for fake products, but it can also be malicious and trick users into opening tainted attachments or visiting malicious websites.

True or false? Spam filtering is only performed on incoming email.

Answer: *False.* Spam filtering can be performed on incoming or outgoing email. Outbound mail filtering is useful to detect if an internal computer has been hacked and is being used to send spam.

Web application firewall vs. network firewall

Whereas network firewalls can be seen as general network devices, web application firewalls are more specialized devices. Web application firewalls are designed specifically to protect web applications against common attacks, such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (XSRF).

True or false? Web application firewalls are designed to detect and block web application attacks.

Answer: *True.* Web application firewalls are very specialized devices. They are designed primarily for ecommerce.

True or false? Network firewalls are specifically designed to detect and prevent SQL injection attacks.

Answer: *False.* Network firewalls are not designed specifically to prevent attacks such as SQL injection.

URL filtering, content inspection, malware inspection

Controlling web traffic is an important task for most security professionals. This includes blocking or granting access to specific URLs. Most organizations will block specific sites that deal with topics such as gambling or pornography. Even though sites titled www.porn.com can be easily blocked, organizations might also want to monitor the content of specific sites and scan for malware.

True or false? URL filtering can be used to provide 100 percent protection and guarantee that users will not go to specific types of websites.

Answer: *False.* Although URL filtering is effective, it is not foolproof. Moreover, sites typically must be added to a list before being filtered.

True or false? Content inspection can be used to look for specific types of content within certain types of webpages.

Answer: *True*. Content inspection is used by many different organizations to look for specific types of web content such as pornography. Upon identifying specific types of content, a site can be flagged or a user might be warned not to revisit the site.

True or false? Malware inspection is a common technique used to detect malicious content such as Trojans and malware.

Answer: *True*. Malware inspection is just one of many techniques used by security professionals to protect internal users from websites that might host malicious content.

Can you answer these questions?

You can find the answers to these questions at the end of this chapter.

1. While using a sniffer program, you have captured some traffic that looks like an active FTP connection. Is it possible that you might be able to see the user name and password in clear text?
2. You currently manage a number of small customers that work from a shared office space. Each is utilizing independent anti-spam, firewall, and antivirus protection. Is there a way for you to centralize these services?
3. There has been a concern in the office over some of the websites that employees are visiting. Is there an easy way for you to deal with this problem and restrict access to specific sites?
4. Which type of intrusion detection system can be used to examine unencrypted network traffic?
5. Can an IDS that monitors network traffic decode encrypted HTTPS traffic?

Objective 1.2: Apply and implement secure network administration principles

In this exam Objective, you might be tested on techniques that are used to implement secure administration principles.

Exam need to know...

- Understand rule-based management

  For example: Can you name the two parts of a firewall–rule-based management?
- Understand how routers can be used to increase security by using access control lists, rules, and secure router configuration

  For example: Can you explain why it is important to communicate securely with the router?

- Describe the various methods by which switches can enhance security, such as flood guards, loop protection, and port security

  For example: Do you know how to use port security to prevent common network attacks?

Rule-based management

Rule-based management is a way to configure firewalls to filter specific types of traffic. The rule base is made up of two parts: the firewall rule, and the action. The firewall rule determines if a specific packet matches the rule criteria. The action defines what happens if the rule is applied. As an example, when a specific packet type is detected, it might be allowed or denied.

True or false? A firewall rule can include a source or destination port.

Answer: *True*. Firewall rules can include source or destination ports, IP addresses, websites, or the service to which it is trying to connect.

True or false? Firewalls process rules in a top-down order.

Answer: *True*. Firewalls typically process rules in a top-down order, moving from first to last.

Firewall rules

Firewall rules are processed in a top-to-bottom order and can be applied to traffic entering or leaving a network. As an example, a firewall rule might be created to only allow web traffic into a network to a specific web server, yet insiders might be allowed to browse external websites.

True or false? Best practice is to start by not allowing any traffic and then allowing only traffic that is approved.

Answer: *True*. A deny-all approach states that no traffic is allowed and that ports and applications are opened on the firewall only as needed.

True or false? Firewall rules typically allow ports 25 and 80 into the network.

Answer: *True*. Port 25 is used for simple mail transfer protocol (email), and port 80 is used for HTTP.

VLAN management

VLAN management allows for the software configuration of end stations to be grouped together, even if they are not located on the same network switch. This allows the grouping of hosts with a common set of requirements to communicate as if they were attached to the same broadcast domain. As an example, accounting, sales, and marketing each can be placed on their own separate VLAN. Even though these devices might be in diverse locations, VLANS allow each group to communicate with others in their VLAN, regardless of their physical location.

> ***EXAM TIP*** **VLANs overcome the geographic concerns of legacy switches so that security professionals can logically group network users without worrying about their geographic or physical location.**

True or false? Switches typically have visual, built-in methods that indicate VLAN port members to personnel who work in a wiring closet.

Answer: *False.* A security professional must typically connect to a switch and look at its configuration to see how the VLANS are configured.

True or false? VLANS operate at Layer 4 of the OSI model.

Answer: *False.* VLANS work at Layer 2 of the OSI model and allow the segmentation of physical traffic.

> ***MORE INFO*** **To learn more about VLAN management, consult the TechNet document at *http://technet.microsoft.com/en-us/library/cc816585%28WS.10%29.aspx*.**

Secure router configuration

Secure router configuration is a key concern for a security professional. Ideally, the configuration should be local, via a console cable. When this is not possible, remote configuration should make use of encryption. Secure Copy Protocol (SCP) is one method to secure remote configuration. When configuring both locally and remotely, it is important to save a backup copy of the configuration so that the router can be easily re-sorted should something go wrong.

True or false? The use of trivial file transfer protocol (TFTP) is acceptable for secure remote configuration of a router.

Answer: *False.* You should use a secure protocol such as SCP. TFTP does not make use of encryption.

Access control lists

The most basic way to configure firewall rules is by means of an access control list (ACL). An ACL is used for packet filtering and for selecting types of traffic to be analyzed, forwarded, and/or influenced in some way by a firewall or other device. Typical, firewalls block traffic based on the source/destination address, port, packet type, and so on. Rules placed in an ACL are used as a form of stateless inspection. Stateless devices look only at a list and make a simple yes/no, allow/disallow decision. ACLs can be used for more than just allowing or blocking traffic. As an example, rules can also log activity for later inspection or to record an alarm.

True or false? An ACL is used for stateful inspection.

Answer: *False.* ACLs are a very basic form of firewall and are considered stateless inspection.

Port security

Port security can mean different things to different people; however, generally it is described as the process of controlling access to ports. This includes physical and logical access. As an example, riser rooms, telecommunication closets, and other areas where there is access to cables, ports, and equipment should be secured. Logical port security can include VLANs, 802.1x, and MAC address filtering.

True or false? Equipment closets should be locked and secured.

Answer: *True.* Even though many IT professionals think of security in terms of logical control, physical control is also critical. Physical security of access points, telecommunication closets, and any other area where cable access is possible should be closely controlled.

802.1x

802.1X is an IEEE standard for port-based Network Access Control. 802.1x is widely used in wireless environments and relies on extensible authentication protocol. 802.1x acts as an application proxy because it acts as a middle man in the authentication process.

True or false? 802.1x makes use of password authentication protocol (PAP).

Answer: *False.* PAP is not used with 802.1x and is considered insecure. 802.1x utilizes extensible authentication protocol (EAP), which offers strong authentication.

> ***MORE INFO*** **To learn more about 802.1x, consult the TechNet document at *http://technet.microsoft.com/en-us/library/cc753354(WS.10).aspx*.**

Flood guards

Flood guards are tools that you can use to prevent Denial-of-Service (DoS) attacks. This technology is typically built in to network equipment such as routers and intrusion prevention equipment. It is designed to detect network floods and then block this traffic. Flood guards help block malicious traffic from entering a network.

True or false? Flood guards are used to prevent broadcast loops.

Answer: *False.* Flood guards are not used to prevent broadcast loops; however, they help to protect against DoS attacks.

True or false? Flood guards detect traffic that is already in the local network and alert the network administrator as to its malicious use.

Answer: *False.* Flood guards are used to block malicious traffic at the edge of a network and prevent it from ever entering an organization's internal domain.

Loop protection

Loop protection is designed to prevent Layer 2 broadcast loops. Loop protection works by sending periodic loop test frames to detect loops within the network cabling. Loop protection can then shut off specific ports to prevent the loops from occurring. Loop protection is typically implemented with spanning tree protocol (STP). STP learns all available paths and then looks for traffic to be looped back.

True or false? Loop protection is implemented on Layer 3 of the OSI model.

Answer: *False.* Loop protection is implemented on Layer 2 of the OSI model because it deals with physical frames. Logical traffic at Layer 3 is prevented from looping by the TTL field in the IP header.

True or false? STP is used to provide loop protection.

Answer: *True.* Ethernet looping is resolved by STP. This unique protocol looks for repeating transmission paths and can work as a filter to block ports, preventing this from occurring.

Implicit deny

Firewall rules are based on an implicit-deny principle: any traffic that is not explicitly allowed by a firewall rule is blocked. This activity is accomplished by the implicit deny-all rule that is logically at the bottom of every firewall rule list. This means the firewall rule set does not explicitly allow a specific type of traffic. If it's blocked, it creates an implicit deny-all.

True or false? By placing a deny-all statement at the beginning of a firewall rule set, you can block all unwanted traffic.

Answer: *False.* There are several common errors made by firewall administrators when setting up a firewall rule, and this is one of them. If you place a deny-all at the beginning of a firewall rule set, you will block all remaining rules and no traffic will be allowed through the firewall.

True or false? If you want to block a specific website, a generic allow-all web traffic rule should be placed before the deny rule that blocks a specific website.

Answer: *False.* Here again is another of the common errors made by firewall administrators. If you place an allow-all statement, all traffic will be passed.

Prevent network bridging by network separation

Years ago, network bridges were widely used because they offered a simple way to separate collision domains. The problem with bridges was that they were slow, introducing latency into a network. Also, bridges offered no security. Today, routers and firewalls are used for network separation. Routers offer the ability to separate the network on Layer 3 of the OSI model and can also provide some security by means of ACLs. Firewalls can offer even more security and can provide deeper packet inspection, allowing for greater control of ingress and egress of traffic.

True or false? Bridges provide logical segmentation.

Answer: *False.* Bridges provide physical segmentation and have the ability to block Layer 2 broadcast traffic.

True or false? Bridges offer multilayer traffic management.

Answer: *False.* Bridges only operate on Layer 2 of the OSI model, whereas routers and firewalls can operate at higher layers. This can provide a much more granular approach to traffic management.

> ***EXAM TIP*** **If you are asked about bridges, keep in mind that they are slower than switches. Switches have a matrix design that allows faster throughput and greater functionality.**

Log analysis

Log analysis is something that is widely discussed and not always properly implemented. Log analysis is the review of audit logs and records. It is considered a detective control because logs are reviewed after the fact. Logs should be moved off of host systems and encrypted for tighter security and to prevent tampering. In many environments, logs may not be reviewed until something goes wrong. Logs should be reviewed periodically to look for anomalies. This can help to reveal problems early on, before they become worse. Logs should be reviewed for configuration errors and signs of malicious activity.

True or false? Log analysis is considered a preventive control.

Answer: *False.* Log analysis is considered a detective control because it is used to uncover errors, problems, and misconfigurations after they have occurred.

True or false? Logs should contain a timestamp and hash.

Answer: *True.* Logs should contain a timestamp and hash to prevent and detect tampering.

> ***EXAM TIP*** **Keep in mind that while users might be quick to tell you when something they need does not work properly, they might not be as quick to tell you that misconfigurations allowed them to access materials or websites that they should not have been accessing.**

Can you answer these questions?

You can find the answers to these questions at the end of this chapter.

1. A new intern has connected all five of the company's switches together into a massive loop, causing a brief broadcast storm. What technology can prevent this from becoming an even bigger problem?
2. You have an RJ-45 port in a meeting room that is accessible by all, but should only be used with one laptop that is assigned to that area. What can you do to prevent other laptops from using the port?
3. You have been tasked with setting up some basic controls to govern what traffic can ingress or egress your network. Is there some way that you can do this on the router?
4. There are many types of controls that a security professional should understand such as preventive, detective, and corrective. What type of control is log analysis?
5. Are bridges considered a smart device?

Objective 1.3: Distinguish and differentiate network design elements and compounds

In this exam Objective, you might be tested on your ability to distinguish and differentiate network design elements and compounds. A security professional must understand how a network functions and what each of the components do. For example, items such as DMZs VLANs, and NACs, all have a specific security purpose. Even items such as remote access and telephony systems must be closely watched to ensure that they are not used inappropriately.

Exam need to know...

- Explain how to deploy a DMZ and what its purpose is

  For example: Do you know that a DMZ resides between the untrusted external network and the internal trusted network?
- The role of subnetting and how it is used to provide segmentation and security

  For example: Do you know that subnetting is used to allocate network addresses into usable blocks?
- Define how network address translation (NAT) is used and its role in providing security and extending the lifespan of IPv4 addresses

  For example: Do you know that NAT provides a level of security by blocking outsiders from seeing the internal structure of a network?
- Discuss remote access and how it is a portal for legitimate users and potential attackers

  For example: Do you know that remote access allows users to access internal resources?
- Detail the purpose of NAC and how it provides greater network security

  For example: Do you know that NAC offers organizations an advanced method of policy enforcement?
- Explain how virtualization is used by most organizations today to better utilize existing resources

  For example: Do you know that virtualization is widely used for development and testing?
- Define cloud computing and identify some related common security concerns

  For example: Do you know that cloud computing offers both advantages and security concerns?

DMZ

Even though the term “DMZ” might conjure up the image of "no-mans land" between North Korea and South Korea, as it relates to networking, it is actually a technical term that describes a special purpose perimeter network which resides between a trusted and untrusted network. The DMZ is designed to allow untrusted

outsiders in to use public access services, such as web, FTP, DNS, and so on. Most DMZs are deployed through the use of a multi-homed firewall via three interfaces. These interfaces include the Internet, an organization's private LAN, and the DMZ.

True or false? A DMZ is used to host public services.

Answer: *True*. Organizations use DMZs to host public services such as web, email, FTP, and DNS. The DMZ allows outsiders limited access to a private network via a specialized security zone.

Subnetting

One advantage of an IP network is that the local portion of the address can be divided into smaller groups. These groups (or subnets) create a more manageable and user-friendly network. Organizations usually create subnets for a combination of reasons that can include:

- Performance problems or high-traffic volume
- Security issues and a need to segment sensitive data
- Connectivity issues and a need to connect distant locations by using a WAN
- The need to connect disparate protocols (for example, Ethernet, Token Ring, Frame Relay, or ATM)

To determine the subnets into which a network has been divided, look at the subnet mask that has been applied. All IP networks use a subnet mask to separate the network portion of the address from the host portion. The subnet mask defines the point at which the network ends and the host begins. The subnet mask is a 32-bit binary number that indicates which portions of a host IP address defines the network ID and which portions define the host ID. As an example, a class A address has an 8-bit mask, a class B address has a 16-bit mask, and a class C address has a 24-bit mask. These are expressed as follows:

- **Class A** 255.0.0.0
- **Class B** 255.255.0.0
- **Class C** 255.255.255.0

Using class C as an example, the first 24 bits of the subnet mask are used to identify the Internet-unique part of the address. To determine the number of subnets into which a network has been divided, look at the subnet mask that has been applied. Table 1-1 shows an example.

TABLE 1-1 Example of Network Subnet

Item	Details
IP address	200.199.21.64
Decimal subnet mask	255.255.255.240
Binary subnet mask	11111111.11111111.11111111.11110000
Bit meaning	14 subnets/14 hosts per subnet

EXAM TIP **If you are not comfortable with subnetting, consult Network+ study materials or search for content online at *http://technet.microsoft.com/en-us/library/bb726997.aspx*.**

True or false? The natural mask for a class A network is 255.255.0.0.

Answer: *False.* The natural mask for a class A network is 255.0.0.0. Whereas a class A network can use a 255.255.0.0, it would mean that the network has been subnetted.

True or false? You cannot subnet a class C network.

Answer: *False.* A class C network can be subnetted. For example, a class C network with a 255.255.255.340.0 mask would have 14 subnets, with 14 usable host addresses on each subnet.

MORE INFO **For a more detailed overview of subnetting, consult the TechNet document at *http://technet.microsoft.com/en-us/library/cc958832.aspx*.**

VLAN

VLANs originated as a security and traffic control that was used to separate network traffic. The VLANs model works by separating its users into workgroups, such as engineering, marketing, and sales. VLANs are created by using switches; they function in much the same way as a subnet because they segment Layer 2 traffic. Security administrators can use VLANs to separate traffic without altering the physical topology. Security administrators also use the functionality of VLANs to block broadcast traffic. Today, many organizations prefer campus-wide VLANs because VLANs have to span and be trunked across the entire network. VLANs block broadcast storms and add security and protection against sniffing.

True or false? VLANS protect against sniffing because each one is treated as a separate subnet.

Answer: *True.* One of the real benefits of a VLAN is its ability to reduce the threat of sniffing. If someone gained access to the accounting department's VLAN and installed a sniffer, he would not see the contents of the VLAN for the sales department.

True or false? Broadcast traffic is evasive because it must be processed by the receiving systems.

Answer: *True.* Broadcast does interrupt the operation of devices because they must pass the data up the stack and evaluate it to see if it must be acted upon. VLANs limit broadcast traffic to only specific segments of the network.

NAT

Network address translation (NAT) was designed to provide a level of security and help to better manage the allocation of IP addresses. Using NAT, an organization can have many internal IP addresses and only one public, external IP address. For example, at your house, you might have 5 to 10 devices connected to your network. Each requires an address, but must they all be public? No, probably not. With NAT,

all these internal devices can use one public IP address. This technology helps better allocate the remaining IPv4 addresses and provides some security, because outsiders cannot directly see your internal address scheme. NAT can use any one of three private address ranges, which include the following:

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

NAT can be deployed as a one-to-one address translation, static address translation, or port address translation (PAT). PAT is one common approach because many internal (private) addresses can share one common public address. The edge device or router knows with which internal device to communicate by tracking ports used and the specific IP address being used for translation.

True or false? If an outsider scans a NAT network, she can directly see the IP address scheme of the internal network.

Answer: *False.* NAT hides the internal address scheme because it is situated between the internal and external network, which prevents outsiders from directly accessing internal systems. The router or NAT device is the only party allowed to maintain a conversation between the external network and the internal private network. NAT maintains a translation table to translate packets to and from the internal and external networks.

True or false? NAT was implemented primarily as a cost-saving measure for ISPs.

Answer: *False.* The true purpose of a NAT is to extend the usability of IPv4–based addresses. Without NAT, every device on an internal network would be required to have a public-addressable IP address. NAT makes it possible to reduce the need for public IP addresses because an end user can have many internal devices, but need only one or even just a few external IP addresses.

True or false? NAT provides some amount of security.

Answer: *True.* With NAT, an outsider cannot directly connect to an internal device. The internal device must request a connection or set up static NAT for a dedicated allowance. Although NAT does not provide a high level of security, it does add one additional layer that prevents an outsider from directly seeing an internal addressing scheme.

MORE INFO **For a more detailed description of NAT, you can reference RFC 2663.**

Remote access

Remote access describes any technology that is used to connect users to remote services. Such systems have historically been used so that users can connect to an organization's servers from other locations via modems and dial-up connections. More recently, remote access servers (RAS) can support modems, VPN links, and terminal services connections. Even though modems are the slowest of the possible connection options, they are still used because of their wide availability. Remote access security can be strengthened by using callback and caller ID. One common

attack against dial-up connections is *wardialing*. Wardialing is a technique by which an attacker dials a large range of numbers and identifies any that connect to a modem. Once identified, this number can be targeted for additional attacks.

True or false? Wardriving is an attack that is used against RAS systems.

Answer: *False*. Wardriving is not an attack against RAS systems. Wardriving is an attack against wireless networks.

True or false? Dial-back is a good defensive measure against unauthorized use of RAS systems.

Answer: *True.* Dial-back is a good defense against unauthorized use of RAS. When the user dials in, dial-back authenticates the user by dialing back to a predefined authorized number.

True or false? RAS can make use of a "plain old telephone service" (POTS) system.

Answer: *True.* POTs is simply a standard phone line that is used for dial-up modem connections on the public switched telephone network (PSTN). Dial-up with the use of modems is the most common RAS type.

> ***MORE INFO*** **For a more detailed description of the RAS process, consult the TechNet document at *http://technet.microsoft.com/en-us/library/cc751039.aspx*.**

Telephony

Telephony was born with the invention of the telephone by Alexander Graham Bell. Telephony can be described as any means to deliver telephone services to an organization or individual. Traditionally, telephony was delivered via POTS lines and modems, but today, telephony also encompasses Voice over IP (VoIP), VPNs, and private branch exchange (PBX).

A PBX is a private telephone system designed for use by businesses and other organizations. Many companies might have one or more public phone lines and might use the PBX to connect these lines to many internal private extensions. The primary issue with PBX is security. A misconfigured PBX can provide the means for malicious user to place free long-distance calls or even alter a PBX configuration or setup. Security professionals should know the basic methods to secure a PBX, which include changing all default passwords, changing access codes, enabling logging and mandating their periodic review, and restricting long-distance calling.

VoIP, although much newer than PBX, also has security vulnerabilities. These include, sniffing, interception, and DoS attacks.

True or false? A PBX system does not present a real security concern.

Answer: *False.* A PBX system is much like other technologies, and it must be secured. One major issue with PBX is toll fraud.

True or false? Outside call routing and call forwarding are not PBX security concerns.

Answer: *False.* Outside call routing and call forwarding are two major PBX issues because both can give an attacker the ability to call in to a PBX and dial out to a

long-distance number. This can cost an organization hundreds or thousands of dollars in long-distance phone charges.

> ***MORE INFO*** **For a more detailed description of PBX and unified communication concerns, consult the TechNet document at *http://technet.microsoft.com/en-us/lync/gg13193*.**

NAC

Network access control (NAC) was developed as a response to the increased need for security that both large and small organizations face. NAC offers administrators a way to verify that devices meet certain "health" standards before they are connected to the network. Laptops, desktop computers, or any device that doesn't comply with predefined requirements are unable to join the network or might even be shunted to a restricted network where access is limited until the device complies with required standards.

There are several different ways to implement NAC. These include infrastructure-based NAC, endpoint-based NAC, and hardware-based NAC. Infrastructure-based NAC requires that an organization upgrade its hardware and/or operating systems. Endpoint-based NAC requires the installation of software agents on each network client. These devices are then managed via a centralized management console. Hardware-based NAC requires the installation of a network appliance. The appliance monitors for specific behavior and can limit device connectivity in the event that non-compliant activity is detected.

True or false? There are two basic ways to implement NAC.

Answer: *False.* There are three basic ways to implement NAC: infrastructure-based NAC, endpoint-based NAC, and hardware-based NAC. Many companies have released NAC products, including Microsoft, Cisco, and Symantec. Each uses one of the three primary approaches.

True or false? The concept of NAC is to control access through strict adherence to and implementation of security policies.

Answer: *True.* The goal of NAC is to aid in the strict control of access policies. For example, an employee's laptop might contain all types of malware upon returning to work after a long weekend. NAC offers administrators a method to verify that devices such as these meet certain health standards before connection to the network.

> ***MORE INFO*** **For a more detailed description of NAC, consult the TechNet document at *http://technet.microsoft.com/en-us/network/bb545879*.**

Virtualization

Virtualization emulates hardware within a *virtual machine* and offers security professionals a means to separate hardware from software. Virtualization duplicates the physical architecture needed for a program or process to function. It is widely used

today with virtual machines. A virtual machine is simply one that is set up as if it has its own hardware, yet it is actually sharing hardware with a physical machine and possibly one or more other virtual machines. CPU, memory, and storage resources are all split between the physical and virtual machine. This approach offers a much better utilization rate for servers while providing the capability to isolate applications and activities. Common examples include Microsoft Virtual PC, Microsoft Virtual Server, Microsoft Hyper-V, VMware, and VirtualBox.

True or false? Virtualization offers faster recovery than traditional physical servers when hardware fails.

Answer: *True*. One of the primary advantages of virtualization is faster recovery. A virtual image can be quickly moved to another physical server and recovered in the event of a hardware failure.

> ***MORE INFO*** **To learn more about Hyper-V, consult the TechNet document at *http://technet.microsoft.com/en-us/library/cc753637(v=ws.10).aspx*.**

Cloud computing

Cloud computing is a business model that delivers computing as a service by providing on-demand access to a pool of computing resources, including software, infrastructure, and hardware facilities, over a network. Some potential cloud computing security concerns can include data protection, identity management, physical security, availability, data privacy, and accountability.

True or false? Cloud computing can be described as a service whereby computing and processing of data is performed elsewhere and not on premises.

Answer: *True*. Cloud computing is often thought of as Internet-based computing, because an organization or individual is using the resources of a third party for data storage, processing, retrieval, or even application services.

> ***MORE INFO*** **To learn more about cloud computing, consult the TechNet document at *http://technet.microsoft.com/en-us/library/gg521165.aspx*.**

Platform as a Service

With Platform as a Service (PaaS), users "rent" hardware, operating systems, storage, and network capacity over the Internet. Using this service delivery model, a customer can purchase virtualized servers and associated services to run existing applications or develop and test new ones.

PaaS involves some risk of "lock-in" if the provider's offerings require proprietary service interfaces or development languages. Another PaaS risk is that the flexibility of offerings might not meet the needs of some users whose requirements evolve rapidly.

True or false? PaaS is a development environment in which a customer can create and develop services on a provider's computing environment.

Answer: *False.* PaaS is actually used for applications so that a customer can create and develop applications on a provider's computing environment.

Software as a Service

Software as a Service (SaaS) is a software distribution model by which applications are hosted by a vendor or service provider and are made available to customers over a network, typically the Internet. With PaaS you are renting hardware to deliver your own private applications, whereas with SaaS, you are using open applications that are provided to all, such as Google Docs and Microsoft Office Online.

SaaS is becoming an increasingly prevalent delivery model because the underlying technologies that support web services and service-oriented architecture (SOA) are continuing to mature and new developmental approaches, such as Ajax, are becoming popular. Benefits of the SaaS model include easier administration, automatic updates, patch management, and global accessibility.

True or false? Microsoft Office 365 and Google Docs are examples of SaaS.

Answer: *True.* Both Microsoft Office Online and Google Docs are examples of Saas. With SaaS, applications are hosted by a cloud provider and made available to customers over the Internet.

MORE INFO **To learn more about using Microsoft Office via the cloud, consult the TechNet document at *http://technet.microsoft.com/en-us/hh456357*.**

Infrastructure as a Service

Infrastructure as a Service (IaaS) is a provision model by which an organization outsources the equipment used to support operations, including storage, hardware, servers, and networking components.

The service provider owns the equipment and is responsible for facilities, operations and maintenance. The client typically pays on a per-use basis.

True or false? IaaS allows companies to scale up internal services by using third-party software.

Answer: *False.* With IaaS, organizations can scale up by using a cloud provider's infrastructure, precluding the need to install massive hardware at their own site.

EXAM TIP **For the exam, you should be able to distinguish between the various types of cloud computing types and services.**

Can you answer these questions?

You can find the answers to these questions at the end of this chapter.

1. Has a Class C network with a 255.255.255.240 mask been subnetted?
2. By which form of cloud-based service do you use someone else's equipment for development?
3. What is the name of a phone system that is used internally and is private to the organization?
4. VMware and Virtual PC are examples of what?
5. What technology is designed to enforce adherence to security policy?

Objective 1.4: Implement and use common protocols

In this exam Objective, you might be tested on how to implement and use common protocols. These can include IPsec, TLS, SSL, IPv4, and IPv6. It is critical for a security professional to understand how these protocols work and what level of security, if any, they provide.

Exam need to know...

- Define what IPsec is used for and what its benefits are

  For example: Do you know that IPsec can be used to protect data in transit?
- The security issues of Simple Network Management Protocol

  For example: Do you know that Simple Network Management Protocol versions 1 and 2 send the community strings via clear text?
- The purpose of Domain Name System and how it is configured

  For example: Do you know that Domain Name System has security vulnerabilities and can be replaced with Domain Name System Security Extensions (DNSSEC)?
- Explain how to use secure solutions such as FTPS, HTTPS, and SFTP to secure network traffic

  For example: Do you know that protection of data in transit is an important concern of security professionals?
- The role of ICMP and how it can be misused

  For example: Do you know that the most common ICMP is ping?
- How IPv4 and IPv6 are used and implemented

  For example: Do you know that IPv6 has integrated IPsec?

IPSec

IPsec is a mandatory part of any IPv6 implementation; with IPv4, it is optional. IPsec can be defined as a solution to the problem of Internet security. IPsec is a suite of protocols used for encrypting data so that you can transmit messages securely over the Internet or private network, send encrypted communications between two

network devices, and secure VPN communications. You can configure IPsec by using either of the following modes:

- **Transport mode** Encrypts only the data portion of the encapsulated packet
- **Tunnel mode** Encrypts both the data and the header portions of the encapsulated packet, hiding more information about the underlying communication

The IPsec protocols comprise four separate security protocols, which can be applied alone or in combination. They include the following:

- **Authentication Header (AH)** The AH protects against malicious modification without providing privacy.
- **Encapsulating Security Payload (ESP)** The ESP header provides privacy and protects against malicious modification.
- **IP Payload Compression Protocol (IPComp)** IPComp reduces the size of IP datagrams by compressing the datagrams to increase the communication performance between two parties.
- **Internet Key Exchange (IKE)** The IKE protocol is a mechanism by which secret keys and other protection-related parameters are exchanged prior to a communication, without the intervention of the user.

True or false? IPsec can be deployed in one of four different modes.

Answer: *False.* IPsec can be deployed in one of two modes: tunnel or transport. Tunnel mode is commonly used to protect traffic between gateways, whereas transport mode is used between end stations that support IPsec.

> ***EXAM TIP*** **For the Security+ exam, you should know the various components of IPsec and what the purpose of each component is.**

True or false? IPsec tunnel mode encrypts only the data portion of the IP packet.

Answer: *False.* Tunnel mode encrypts both the data and header portions of the IP packets.

> ***MORE INFO*** **To learn more about IPsec, consult the TechNet document at *http://technet.microsoft.com/en-us/library/bb726946.aspx*.**

SNMP

Simple Network Management Protocol (SNMP) is a network management protocol based on client/server architecture. SNMP is designed to monitor and manage devices. The agent collects information from the device and holds it in a table while the managers poll agents to gather this data, which they use to present a centralized view of the network to administrators.

SNMP stores all values in a Management Information Base (MIB) table on the managed device. Values are referenced by using a series of dotted integers. The

manager uses the MIBs to define the dotted integers so that data can be reported back by the agent.

Security professionals should be aware of SNMP because it might be installed or running by default or without the security administrator's knowledge. SNMPv1 and SNMPv2 send all information in clear text and use the default community strings, public and private. SNMP can be spoofed and sniffed to extract all sorts of information. SNMPv3 offers encryption, but it is not supported on all devices.

True or false? SNMPv2 offers encryption.

Answer: *False.* SNMPv1 and v2 do not offer encryption. Only SNMPv3 offers encryption.

True or false? SNMP v1 community strings can be sniffed.

Answer: *True.* SNMPv1 and v2 use clear-text community strings, which default to public and private.

True or false? SNMP uses port 389.

Answer: *False.* SNMP uses UDP port 161 and 162.

> ***EXAM TIP*** **Remember that SNMPv1 and v2 are not secure; when possible you should use SNMPv3.**

> ***MORE INFO*** **To learn more about SNMP, consult the TechNet document at *http://technet.microsoft.com/en-us/library/bb726977.aspx*.**

SSH

Secure Shell (SSH) is a replacement for the Berkeley "r" utilities and for applications such as FTP and Telnet. SSH can be used to securely access a remote computer. It operates on TCP port 22.

True or false? SSH uses port 21 by default.

Answer: *False.* The default port for SSH is TCP port 22.

> ***EXAM TIP*** **Remember that applications such as FTP and Telnet are considered vulnerable. Secure applications such as SSH should be used whenever possible.**

> ***MORE INFO*** **To learn more about running SSH from the command line, consult the TechNet document at *http://technet.microsoft.com/en-us/library/gg440664.aspx*.**

DNS

Domain Name System (DNS) serves the critical function of address translation by converting fully-qualified domain names (FQDNs) into a numeric IP address, and vice versa. This application operates on port 53 (TCP and UDP). If the DNS were to fail, the Internet would continue to function, but it would require that Internet users

knew the IP address of every site to which they want to visit. Of course, this means that for all practical purposes, the Internet would not be useable without the DNS. The DNS database consists of one or more zone files. Each zone is a collection of structured resource records. Common record types include the Start of Authority (SOA) record, A record, CNAME record, NS record, PTR record, and the MX record. There is only one SOA record in each zone database file; it describes the zone name space. The A record is the most common because it contains IP addresses and names of specific hosts. The CNAME record is an alias. The NS record lists the IP address of other name servers. An MX record is a Mail Exchange record. This record has the IP address of the server where email should be delivered. Hackers can target DNS for many types of attacks. One such attack is DNS *cache poisoning*. This type of attack sends fake entries to a DNS server to corrupt the information stored there. DNS can also be susceptible to DoS attacks and to unauthorized zone transfers. DNS uses UDP for DNS queries and TCP for zone transfers.

True or false? DNS can use both TCP and UDP.

Answer: *True.* DNS is one of the few protocols that can use both TCP and UDP. DNS typically uses UDP for record lookups and TCP for zone transfers.

True or false? An MX record is used for replication.

Answer: *False.* An MX record is associated with the mail server. The MX records specifies how email should be routed by using the Simple Mail Transfer Protocol.

> ***MORE INFO*** **To learn more about how DNS works, consult the TechNet document at *http://technet.microsoft.com/en-us/library/cc775637(v=ws.10).aspx*.**

TLS

Transport Layer Security (TLS) is the updated version of SSL. Although SSL and TLS do basically the same thing, they are implemented slightly different. What both share in common is their use of both symmetric and asymmetric algorithms. TLS uses more secure cryptographic protocols and algorithms.

True or false? TLS make use of both symmetric and asymmetric encryption.

Answer: *True.* TLS uses hybrid encryption, which means that it uses symmetric encryption for data and asymmetric encryption for key exchange of the symmetric key.

> ***MORE INFO*** **To learn more about the differences between TLS and SSL, consult the TechNet documents at *http://technet.microsoft.com/en-us/library/cc784450(v=WS.10).aspx*.**

SSL

Secure Sockets Layer (SSL) was developed to secure application data as it travels over the Internet. It was developed by Netscape, and at the time of its release, it set

the standard for Internet security. SSL uses hybrid encryption. It operates in a 40-bit and 128-bit mode, and follows these steps during the communication process:

1. The client requests the use of SSL.
2. The server responds to the request with its X.509 certificate, the name of its certificate authority, and the public key.
3. The server's certificate is verified by the client and a symmetric session is generated. This key is encrypted with the server's public key and sent to the server.
4. The server decrypts the session key and sends a report of the session details to the client, encrypted with the session key.
5. The client reviews the summary and sends its own summary back to the server, likewise encrypted with the session key.
6. After both entities receive a matching session summary, secured SSL communications are initiated.

True or false? SSL has been replaced with TLS.

Answer: *True.* Although both protocols basically serve the same purpose, TLS is the updated version. TLS 1.0 and SSL 3.0 are not interchangeable.

TCP/IP

TCP/IP is the foundation of all modern networks. In many ways, you could say that it has grown up along with the development of the Internet. Originally, the TCP/IP model was developed as a flexible, fault-tolerant set of protocols that were robust enough to avoid interruption in the event that one or more nodes fail. After all, the forerunner to the Internet, the ARPANET, was designed to withstand a nuclear strike (which would likely destroy key routing nodes). The designers of this original network never envisioned the Internet as we know it today. Because TCP/IP was designed to work in a trusted environment, many TCP/IP protocols are now no longer considered secure. Little concern was ever given to the fact that an untrusted party might have access to the wire and be able to sniff the clear-text password. Most networks today, run TCP/IPv4. Many security mechanisms in TCP/IPv4 are add-ons to the original protocol suite.

True or false? TCP/IP was designed with security in mind.

Answer: *False.* TCP/IP was designed with functionality in mind; it was not originally focused on security. Many security features to TCP/IP have been added on, such as IPsec.

FTPS

FTP Secure (FTPS) is a secure version of FTP that integrates SSL. FTPS is not the same as SSH File Transfer Protocol (SFTP). These two protocols are incompatible because the latter uses the Secure Shell (SSH) protocol. FTPS supports two basic modes, Explicit and Implicit, that were developed to invoke client security for use with FTP clients.

Implicit mode suggests that the client must specifically challenge the FTPS server with a TLS/SSL Client Hello message. This assumes that only FTPS clients will connect. Explicit mode (FTPES) requires that an FTPS client must explicitly request security from an FTPS server and then step up to a mutually agreed encryption method.

True or false? FTPS is interchangeable with FTP.

Answer: *False.* FTP and FTPS are different protocols. Each requires unique ports and applications with which to interact.

> ***EXAM TIP*** **Remember that FTPS can support both the Explicit or Implicit modes for use with FTP clients.**

> ***MORE INFO*** **To learn more about FTPS, consult the TechNet document at *http://forums.iis.net/t/1150787.aspx*.**

HTTPS

Although HTTP (port 80) is the standard of the Internet, it does not use encryption or offer anything in the way of security. Luckily, there are some add-ons to HTTP that can be used to increase security. One of the primary add-ons is Hypertext Transfer Protocol Secured (HTTPS). HTTPS (port 443) strengthens HTTP by incorporating SSL or TLS. Some Microsoft products remap port 443 to 4443 on the internal side. These security protocols allow for the use of encryption. You can see when they are in use because the URL begins with HTTPS and a padlock icon appears in the status bar or browser bar in the browser window. HTTPS is the worldwide standard that is used for payment transactions and for other data-sensitive Internet transactions.

True or false? HTTP is sufficient for sensitive transactions.

Answer: *False.* HTTP sends all information in clear text; HTTPS should be used for secure communication.

> ***MORE INFO*** **To learn more about HTTPS, consult the TechNet documents at *http://technet.microsoft.com/en-us/library/cc736680(v=WS.10).aspx*.**

SFTP

Secure FTP (SFTP) should be used because of the inherent insecurities of FTP. FTP sends all data in the clear and offers no protection from password sniffing or data interception. FTP uses TCP ports 20 and 21. SFTP addresses the FTP security issues by encrypting both logon and data communications, which prevents passwords and sensitive data from being transmitted in the clear. Although SFTP is similar to FTP, it uses a different command set and cannot be used with standard FTP client software.

True or false? SFTP and FTP share the same command set.

Answer: *False.* Even though SFTP and FTP can use the same ports, they use a different set of commands and are incompatible.

SCP

Secure Copy Protocol (SCP) is another example of a secure file transfer protocol that can be used as a replacement for FTP. Linux systems commonly use SCP, although Windows versions are available. SCP is based on SSH, and SSH is commonly used as a command-line tool; however, there are some Windows GUI file transfer clients available.

True or false? SCP is similar to SSH.

Answer: *True*. Both SSH and SCP use the same command set and are very similar. SCP can be used as a replacement for FTP because it offers much greater security.

> ***EXAM TIP*** **Remember that there are many replacements for FTP, such as SCP, SFTP, and FTPS. Each offers much greater protection of network traffic than FTP.**

ICMP

Internet Control Message Protocol (ICMP) provides feedback that you can use for diagnostics or to report logical errors. The most common ICMP type is the ping. The designers of ICMP envisioned a protocol that would be helpful and informative. Unfortunately, hackers have a different vision; they use ICMP to send the *ping of death*, craft *Smurf* DoS packets, query the timestamp of a system or its netmask, or even send ICMP type 5 packets to redirect traffic. Loki is an ICMP attack tool that uses ICMP as an encapsulation or tunnel protocol. Some common ICMP types and codes are shown in Table 1-2.

TABLE 1-2 ICMP Codes

Type	Code	Function
0/8	0	Echo response/request (Ping)
3	0–15	Destination unreachable
4	0	Source quench
5	0-3	Redirect
11	0–1	Time exceeded
12	0	Parameter fault
13/14	0	Timestamp request/response
17/18	0	Subnet mask request/response

True or false? A source quench is one of the most common ICMP message types.

Answer: *False*. One of the most common ICMP types is a ping. Ping is a common tool that is used to verify connectivity.

True or false? Oversized pings can be used to launch DoS attacks.

Answer: *True*. Several DoS attacks have been developed that use ping, such as the ping of death and Smurf.

MORE INFO **To learn more about how to block and unblock ICMP traffic, consult the TechNet document at *http://technet.microsoft.com/en-us/library/cc786463(v=WS.10).aspx*.**

IPv4 vs. IPv6

Internet Protocol (IP) is really the engine of the Internet. IP is a routable protocol that is used for addressing and transporting data across a network or the Internet. There are two versions of IP that Security+ candidates should understand: IPv4 and IPv6. IPv4 uses a 32-bit addressing scheme to make "a best effort at delivery." IPv4 composes addresses in a four-decimal–number format. Each of these decimal numbers is one byte in length to allow numbers to range from 0–255. IPv6 uses a 128-bit address, has a simpler header format, eliminates broadcast traffic, and has built-in support for IPsec. IPv6 is the replacement for IPv4 because the IPv4 address space has been depleted. However, it will probably still be a few years before IPv6 makes a significant impact on the Internet.

MORE INFO **To learn more about how IPv6 works, consult the TechNet document at *http://technet.microsoft.com/en-us/library/cc781672(v=WS.10).aspx*.**

True or false? IPv4 uses an 8-bit address.

Answer: *False.* IPv4 uses a 32-bit address and IPv6 uses a 128-bit address. The move to IPv6 will accommodate many more usable addresses in the years to come.

Can you answer these questions?

You can find the answers to these questions at the end of this chapter.

1. Which component of IPsec provides privacy and protects against malicious modification?
2. Which version of IP uses a 32-bit address?
3. What is another name for an ICMP 0/8 message?
4. Which security service was originally developed by Netscape and is application independent?
5. Which DNS record acts as an alias?

Objective 1.5: Identify commonly used default network ports

In this exam Objective, you might be tested on what applications use specific ports. You do not need to memorize all 65,000 potential ports for the exam, but you will need to know common ports and protocols.

Exam need to know...

- FTP uses port 21 for command and control
  For example: Do you know that FTP sends information in the clear?

- SFTP uses TCP as a transport protocol
  For example: Do you know that SFTP is a secure version of FTP?
- TFTP used UDP as a transport
  For example: Do you know that TFTP does not use a user name or password?
- Telnet is considered an antiquated protocol
  For example: Do you know that Telnet is not considered secure?
- SSH is a secure version of the Berkeley "r" utilities
  For example: Do you know that SSH is a good replacement for Telnet?
- NetBIOS can use several ports for communication and use both TCP and UDP as a transport protocol
  For example: Do you know that common NetBIOS ports include 135 and 139?

FTP

FTP uses TCP as a transport. It makes a connection on port 21 and moves data on port 20. Security administrators should carefully configure FTP servers that allow anonymous access. Many FTP servers have anonymous FTP enabled; thus, to limit access to authenticated users only, it must be specifically disabled.

One basic security control is blind FTP. This capability means that when files are uploaded, they are unreadable by visitors. Even if a user knows the exact pathname and name of a file, reading or downloading it is not possible. This helps to add some level of security to an FTP site.

True or false? FTP is an acceptable protocol and found on many networks.

Answer: *False.* FTP is considered antiquated in that it sends information via clear text. It should be replaced with more secure protocols such as SSH.

MORE INFO **To learn more about FTP, consult the TechNet document at *http://technet.microsoft.com/en-us/library/dd421710(v=WS.10).aspx*.**

SFTP

SFTP is a secure version of FTP that uses TCP port 22.

True or false? SFTP uses port 22 by default.

Answer: *True.* There are about 65,000 ports. Well-known services use default ports, and the default port for SFTP is TCP port 22.

FTPS

FTPS is another secure version of FTP. It makes use of SSL. FTP over SSL uses TCP port 990 for control and TCP port 989 for data communication.

True or false? SFTP uses port 20 and 21.

Answer: *False.* SFTP does not use the same ports and FTP. It uses ports 989 and 990.

TFTP

Trivial FTP (TFTP) is a stripped down version of FTP that requires no user name and password and offers no security. TFTP does not provide file listings or information as to what is in remote folders. TFTP is still widely used for router configurations. It uses UDP port 69.

True or false? TFTP can be secured by setting a strong user name and password.

Answer: *False.* TFTP does not use a user name and password; it is not considered secure.

TELNET

Telnet is another antiquated protocol. It functions as a TCP service that operates on port 23. Telnet enables a client at one site to establish a session with a host at another site. The program passes the information typed at the client's keyboard to the host computer system. Although Telnet can be configured to allow anonymous connections, it should be configured to require user names and passwords. Unfortunately, even then, Telnet sends them in clear text. When a user is logged on, he can perform any allowed task. Applications such as SSH should be considered as a replacement.

True or false? Telnet uses UDP port 23.

Answer: *False.* Telnet uses TCP port 23.

HTTP

HTTP is a TCP service that operates on TCP port 80. This is one of the most well-known applications. HTTP has helped make the web the popular protocol that it is today. The HTTP connection model is known as a stateless connection. HTTP uses a request response protocol in which a client sends a request and a server sends a response. Attacks that exploit HTTP can target the server, browser, or scripts that run on the browser.

True or false? HTTP provides basic protection for sensitive data.

Answer: *False.* HTTP sends information in clear text and is not suitable for sensitive data. In those situations, HTTPS should be used.

HTTPS

HTTPS uses TCP port 443 or TCP port 80 in some configurations of TLS.

True or false? HTTPS uses TCP for communication.

Answer: *True.* HTTPS uses TCP for a transport protocol.

> ***MORE INFO*** **To learn more about the differences in HTTP and HTTPS, consult the TechNet document at *http://blogs.msdn.com/b/securitytipstalk/archive/2011/04/04/http-vs-https-what-s-the-difference.aspx*.**

SCP

SCP is another secure alternative to FTP. It uses TCP port 22.

True or false? Both FTP and SCP use the same ports.

Answer: *False*. FTP uses port 20 and 21; SCP uses port 22.

SSH

SSH uses TCP port 22.

True or false? SSH was originally designed as a replacement to Telnet.

Answer: *False*. SSH was originally designed as a replacement to the Berkeley "r" utilities.

NetBIOS

Network Basic Input/Output System (NetBIOS) allows applications on separate systems to communicate over a LAN. There are several components to NetBIOS. NBT (NetBIOS over TCP/IP) uses UDP port 137; NetBIOS Session service uses TCP port 139; and NetBIOS Datagram service uses UDP port 138. The NetBIOS name is up to 16 characters long, and in Windows, it is separate from the computer name. This name is used to identify the computer.

True or false? NetBIOS is comprised of three distinct services.

Answer: *True*. There are several components to NetBIOS. NBT (NetBIOS over TCP/IP) uses UDP port 137, NetBIOS Session service uses TCP port 139, and NetBIOS Datagram service uses UDP port 138.

> ***MORE INFO*** **To learn more about NetBIOS and TCP, consult the TechNet document at *http://technet.microsoft.com/en-us/library/cc940063.aspx*.**

Can you answer these questions?

You can find the answers to these questions at the end of this chapter.

1. What port does FTP use for data exchange?
2. You have used a port scanning tool to scan a network host. You have found port 22 open on a Linux server. What program typically uses this port?
3. What protocol does TFTP use?
4. You have been asked to open up a port on the firewall to let HTTP traffic in. What port and protocol should you configure?
5. You have been asked to open port 443 on the firewall; what application uses this port?

Objective 1.6: Implement wireless networks in a secure manner

In this exam Objective, you might be tested on how to implement wireless in a secure manner. Wireless is an important topic because it is all around us. Organizations and individuals use it at home, work, and when traveling. Therefore, securing it is of the utmost importance.

Exam need to know...

- Describe common wireless LAN vulnerabilities and how you can deal with them

  For example: Do you know that unencrypted wireless offers attackers easy access to a network?
- WEP was developed to protect wireless connections

  For example: Do you know that WEP has been broken?
- WPA is an improvement to WEP and is backward compatible

  For example: Do you know that WPA was designed to overcome the weakness of WEP?
- WPA2 is the newest form of wireless protection, using of a 265-bit key

  For example: Do you know that WPA2 is the newest form of wireless protection?
- Explain how MAC filtering is used

  For example: Do you know that MAC filtering can be used to block or allow devices based on their MAC address?

WPA

Wi-Fi Protected Access (WPA) is the successor to WEP. WPA delivers a level of security far beyond that offered by WEP. It was a temporary fix until the new 802.11i amendment was approved. WPA uses Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys by using a hashing algorithm and adds an integrity-checking feature that verifies that the keys haven't been tampered with. WPA improves on WEP by increasing the Initialization Vector (IV) from 24 bits to 48. Rollover has also been eliminated, which means that key reuse is less likely to occur. WPA also avoids another weakness of WEP by using a different secret key for each packet. Another improvement in WPA is message integrity. WPA addressed a message integrity check (MIC) that is known as Michael. Michael is designed to detect invalid packers and can even take measures to prevent attacks.

True or false? WPA is a totally secure solution to wireless communication.

Answer: *False.* WPA is an improvement to WEP, but it is not fully secure. It uses TKIP and employs a secret passphrase.

MORE INFO **To learn more about wireless deployment best practices, consult the TechNet document at *http://technet.microsoft.com/en-us/library/bb457091.aspx*.**

WPA2

In 2004, the IEEE approved the next upgrade to wireless security: WPA2. It is officially known as 802.11.i. This wireless security standard makes use of the Advanced Encryption Standard (AES) and Cipher Block Chaining Message Authentication Code Protocol (CCMP). Key sizes of up to 256 bits are now available, which is a vast improvement from the original 40-bit encryption that WEP used.

True or false? 802.11.x and WPA2 are indeed different names for the same protocol.

Answer: *False*. 802.11.i and WPA2 are different names for the same protocol. 802.11.x is a standard for port-based authentication.

WEP

The original security mechanism for wireless networks was Wired Equivalent Privacy (WEP). This protocol was developed to address the basic security issues of a wireless network and provide at least the same level of protection as that offered by a wired network. WEP is based on the RC4 symmetric encryption standard and uses either a 64-bit or 128-bit key. WEP makes use of a 24-bit IV to provide randomness. So, the "real key" is actually 40 or 104 bits long. There are two ways to implement the key. First, there is the default key method, which shares a set of up to four default keys with all of the wireless APs. Second is the key mapping method, which sets up a key-mapping relationship for each wireless station with another individual station. This method offers slightly more security, but it entails more work. Consequently, most WLANs use a single shared key on all stations, which makes it easier for a hacker to recover the key. WEP was cracked almost as soon as it was released; in fact, it can be easily cracked in less than five minutes. Luckily, there are replacements to WEP, such as WPA and WPA2.

True or false? WEP uses an asymmetric algorithm.

Answer: *False*. WEP uses RC4, which is a symmetric algorithm.

True or false? In WEP, RC4 was weakened by using 20 bits for an IV.

Answer: *False*. RC4 was weakened, but the IV is 24 bits. This reduced the key size to either 40 or 104 bits.

EAP

Extensible Authentication Protocol (EAP) is an authentication framework that is used in wireless networks. EAP defines message formats and then leaves it up to the protocol to define a way to encapsulate EAP messages within that protocol's message. There are many different EAP formats in use, including EAP-TLS, EAP-PSK, and EAP-MD5.

True or false? EAP is a specific authentication mechanism.

Answer: *False.* EAP is not a specific mechanism of authentication; rather, it is an authentication framework.

> ***MORE INFO*** **For more information about EAP, consult the TechNet document at *http://technet.microsoft.com/en-us/network/bb643147*.**

PEAP

Protected Extensible Authentication Protocol (PEAP) encapsulates EAP within a secure tunnel. The purpose for this was to correct deficiencies in EAP. PEAP provides authentication and encryption. PEAP was jointly developed by Microsoft, RSA Security, and Cisco Systems. PEAP makes use of TLS and corrected the security issue of unencrypted EAP communications.

> ***MORE INFO*** **To learn more about PEAP, consult the TechNet document at *http://technet.microsoft.com/en-us/library/cc754179.aspx*.**

True or false? PEAP was developed as a Microsoft-specific solution.

Answer: *False.* PEAP was developed by Microsoft, Cisco Systems, RSA Security, and others as an open standard. PEAP tunnels traffic by using TLS.

LEAP

Lightweight Extensible Authentication Protocol (LEAP) provides user name/password–based authentication between a wireless client and a RADIUS server. LEAP is a Cisco alternative to TKIP that was developed to overcome existing vulnerabilities.

LEAP provides security by using a dynamic key delivery. This eliminates static key vulnerabilities. However, LEAP has been found to be vulnerable to certain attacks such as man-in-the-middle attacks and session hijacking. EAP-TLS is seen as an acceptable alternative.

True or false? LEAP was developed to address issues with PEAP.

Answer: *False.* PEAP was developed to address issues with TKIP. PEAP was created before the 802.11i/WPA2 system was ratified as a standard.

> ***MORE INFO*** **To learn more about LEAP, consult the TechNet document at *http://social.technet.microsoft.com/Forums/nl-NL/w7itpronetworking/thread/fe4cfb32-954c-4562-a0fc-1e623b5bfa5e*.**

MAC filtering

Another potential security measure that might work, depending on the organization, is to limit access to the wireless network to specific network adapters; some switches and wireless access points have the ability to perform media access control (MAC) filtering. MAC filtering uses the MAC address assigned to each network

adapter to enable or block access to the network. Probably one of the easiest ways to raise the security of the network is to retire your WEP devices. As discussed earlier in this chapter, no matter what the length of the key, WEP is vulnerable. Moving to WPA makes a big improvement in the security of your wireless network. Be aware, however, that using WEP or WPA will not prevent an attacker from sniffing the MAC addresses, because that information is sent in the clear.

True or false? MAC address filtering can be used to prevent all hackers from gaining access to a wireless network.

Answer: *False.* MAC address filtering can be used to help prevent hackers or others from accessing your network, but it is not 100 percent secure. MAC addresses can be sniffed and spoofed, allowing an attacker to bypass MAC address filtering.

> ***MORE INFO*** **To learn more about why MAC address filtering is not a strong security control, consult the following document at *http://www.zdnet.com/blog/ou/the-six-dumbest-ways-to-secure-a-wireless-lan/43*.**

SSID broadcast

The service set identifier (SSID) is a 32-character unique identifier that acts as a network name and is used to identify the wireless network to specific devices. All devices attempting to connect to a specific wireless access point must use the same SSID. The SSID is used to differentiate one wireless network from another. Because the SSID can be sniffed, it does not supply any security to the network. Some security professionals set it to a non-broadcast mode; however, disabling the SSID only obscures the network, because the SSID is still needed. It is still discoverable with a wireless packet sniffer.

True or false? An SSID acts as a strong password.

Answer: *False.* An SSID is more like an identifier than a password. The SSID is broadcast on a regular basis within a special packet known as the beacon frame. This can be disabled to make it more difficult for an attacker to find the wireless network.

> ***MORE INFO*** **To learn more about SSID broadcasts, consult the TechNet document at *http://blogs.technet.com/b/networking/archive/2008/02/08/non-broadcast-wireless-ssids-why-hidden-wireless-networks-are-a-bad-idea.aspx*.**

TKIP

Temporal Key Integrity Protocol (TKIP) was designed as a replacement to WEP that doesn't require a hardware upgrade. TKIP scrambles the keys by using a hashing algorithm and adds an integrity-checking feature that verifies that the keys haven't been tampered with. TKIP added security to WEP by implementing a key mixing function that combines the secret root key with the initialization. It also implemented a sequence counter to protect against replay attacks and added a 64-bit Message Integrity Check (MIC).

True or false? TKIP was designed as a replacement for WPA.

Answer: *False.* TKIP was actually designed as a replacement for WEP and was implemented under the WPA standard.

CCMP

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) is an encryption protocol designed to replace wireless products that use WEP. CCMP was designed to address the vulnerabilities found in TKIP. It uses AES (Advanced Encryption Standard) with a 128-bit key. CCMP provides data confidentiality, authentication, and access control.

True or false? CCMP uses RC4 and supports a 40 or 104-bit key.

Answer: *False.* CCMP uses AES with a 128-bit key.

> ***MORE INFO*** **To learn more about CCMP and secure wireless configuration, consult the TechNet document at *http://technet.microsoft.com/en-us/library/cc875845.aspx*.**

Antenna placement

In certain situations, you might find it necessary to alter the placement of an antenna. It might be that clients near the edge of reception sometimes have problems maintaining a connection, or that walls, beams, or supports are blocking wireless signals. The best approach when placing an antenna is to find a central location that is free of physical obstructions. You will also want to place it at a distance from other devices that can cause interference, such as cordless phones and microwave ovens. Even when a site seems suitable, don't decide on it prematurely. Test the signal strength of various devices before permanently mounting the antenna. You should also consider the signal emanation outside the building.

True or false? Wireless antennas are not affected by reflective or flat metal surfaces.

Answer: *False.* Wireless antennas are affected by many types of obstructions, including reflective or metal surfaces.

Power level control

With some wireless APs, you can manually adjust the power or allow a user to change antennas. These are typically altered after a site survey has been performed or a determination that power levels are too high or low. For situations in which walls or other barriers are present, the user might want to increase power to deal with these forms of interference. For other situations in which bleed-over is a problem, you might want to decrease the power level to reduce the range of the AP. Regardless of what changes you make, be sure to initially note the settings on the device so that you can easily revert to the default value, if needed.

True or false? Power level controls should always be set to the maximum possible value.

Answer: *False.* Power level controls should be set high enough to maintain connection with all devices, which might not necessitate maximum power.

MORE INFO **To learn more about properly configuring wireless access controls, consult the TechTarget document at *http://searchnetworkingchannel.techtarget.com/tip/How-to-configure-wireless-access-points*.**

Can you answer these questions?

You can find the answers to these questions in the section that follows.

1. What encryption algorithm is used by WEP?
2. What protocol was designed as a backward replacement to WEP?
3. What is the maximum key size in WPA2?
4. What are three benefits that CCMP provides?
5. Is EAP an improved wireless messaging format?

Answers

This section contains the answers to the "Can you answer these questions?" sections in this chapter.

Objective 1.1: Explain the security function and purpose of network devices and technologies

1. Yes, sniffers can capture many types of traffic, including unencrypted FTP traffic. This includes clear text, user name, and password.
2. You could choose to use an all-in-one device. Typically, these devices reside at the edge of a network and serve multiple purposes, such as SPAM detection, firewall, and virus detection.
3. URL filtering can be used to deal with this issue. URL filtering can be used to block specific sites that might contain objectionable content such as pornography and gambling.
4. NIDS are used to capture and analyze network traffic. This form of intrusion detection is widely used and typically deployed with sensors in various locations such as in the DMZ, at the gateway, and in the internal network.
5. While NIDS are very useful, they do have limits just like any security tool. NIDS can see encrypted traffic but cannot decrypt it or examine the contents.

Objective 1.2: Apply and implement secure network administration principles

1. The broadcast storm stopped because of loop protection. Loop protection functions by looking for loops in networks and blocking one of the ports to prevent the loop from occurring.

2. Use port security. With port security, you can filter allowed devices by MAC address. Only approved MAC addresses can connect to and use the active port.
3. Yes, you can use an ACL. With the ACL, you can set basic controls on the type of traffic that can ingress or egress your network.
4. Log analysis is a detective control because it is reviewed after the event.
5. Bridges are considered dumb devices. Switches are smarter and faster. They have replaced bridges in almost all networks.

Objective 1.3: Distinguish and differentiate network design elements and compounds

1. A natural mask for a class C network is 255.255.255.0. Any value in the last octet besides a zero indicates that it has been subnetted.
2. PaaS is a way to rent hardware, operating systems, storage, and network capacity over the Internet.
3. A PBX is a private telephone system designed for use by a company or business. Many companies might have one or more public phone lines and might use the PBX to connect this to many internal private extensions.
4. Virtualization. Common examples include VMware, Virtual PC, Virtual Server, Hyper-V, and VirtualBox.
5. NAC is designed to enforce adherence to security policy.

Objective 1.4: Implement and use common protocols

1. The Encapsulating Security Payload (ESP) header provides privacy and protects against malicious modification.
2. IPv4 uses a 32-bit address and is being phased out and replaced with IPv6.
3. The ping. Ping is the most common type of ICMP message.
4. SSL was developed to secure application data while in transit over the Internet. It was developed by Netscape and set the standard for Internet security at the time of its release. SSL makes use of hybrid encryption.
5. This CNAME record is an alias.

Objective 1.5: Identify commonly used default network ports

1. FTP uses port 20 for data exchange.
2. On Linux systems, SSH typically uses port 22.
3. TFTP uses UDP for a transport protocol.
4. HTTP uses TCP port 80.
5. HTTPS uses port 443.

Objective 1.6: Implement wireless networks in a secure manner

1. WEP used RC4 and an encryption algorithm.
2. WPA improved on WEP and made use of a 48-bit IV that does not repeat or roll over.
3. WPA2 uses AES and can support a 256-bit key.
4. CCMP provides data confidentiality, authentication, and access control.
5. EAP is an authentication framework.

Index

Symbols

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

About the Author

Michael Gregg is COO of Superior Solutions, Inc. (*www.thesolutionfirm.com*), a Houston-based information security assessment, penetration testing, and IT security training firm. Mr. Gregg is responsible for helping corporations establish and validate enterprise-wide information security programs and controls. He is an expert on cyber security, networking, and Internet technologies. Even though consulting consumes a large amount of Michael's time, he has contributed to more than 10 books and has spoken at security, technology, and educational conferences such as ISC2's Security Leadership Conference, Hacker Halted, Government Technology Conference (GTC), National Credit Union Administration (NCUA) IT Conference, and The American College of Forensic Examiners.

Michael has appeared in numerous media outlets including *The New York Times*, Fox News, Canadian News (BNN), *Kiplinger*, as well as NPR, ESPN, and other major networks. He holds two associate's degrees, a bachelor's degree, and a master's degree. He presently maintains many certifications, including CISSP, CISA, CISM, and more.

What do you think of this book?

We want to hear from you!

To participate in a brief online survey, please visit:

microsoft.com/learning/booksurvey

Tell us how well this book meets your needs—what works effectively, and what we can do better. Your feedback will help us continually improve our books and learning resources for you.

Thank you in advance for your input!

Microsoft® Press