Лекция 8

Угрозы, уязвимости и основные механизмы защиты сетей

Угрозы и уязвимости сетей

Самыми частыми и опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки пользователей, операторов и системных администраторов, обслуживающих корпоративные информационные системы.
Иногда такие ошибки приводят к прямому ущербу (неправильно введенные данные, ошибка в программе, вызвавшая остановку или разрушение системы). Иногда они создают слабые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования).

Согласно данным Национального института стандартов и технологий США (NIST) 55% случаев нарушения безопасности ИС - следствие непреднамеренных ошибок. Работа в глобальной информационной сети делает этот фактор достаточно актуальным, причем источником ущерба могут быть действия как пользователей организации, так и пользователей глобальной сети, что особенно опасно.

Угрозы и уязвимости сетей

На втором месте по размерам ущерба располагаются кражи и подлоги. В большинстве расследованных случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и защитными мерами. Наличие мощного информационного канала связи с глобальными сетями при отсутствии должного контроля за его работой может дополнительно способствовать такой деятельности.

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны вредить весьма эффективно. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа к информационным ресурсам аннулировались.

Преднамеренные попытки получения несанкционированного доступа через внешние коммуникации занимают в настоящее время около 10% всех возможных нарушений.

Угрозы и уязвимости сетей

Источники нарушений безопасности в корпоративной информационной системе:

1. Ошибки пользователей и персонала – 55%;

2. Проблемы физической безопасности – 15%;

3. Атаки извне – 10%;

4. Нечестные сотрудники – 10%;

5. Обиженные сотрудники – 6%;

6. Вирусы – 4%.

Угрозы и уязвимости сетей

Как правило угрозы сетям перечисляют, по сути сваливая в кучу:

I. Технические угрозы:
1. Ошибки в программном обеспечении.
2. Различные DoS- и DDoS-атаки.
4.Угрозы безопасности информации при работе в открытых беспроводных сетях Wi-Fi
5. Анализаторы протоколов и прослушивающие программы («снифферы»).
6. Технические средства съема информации.

II. Человеческий фактор:
1. Уволенные или недовольные сотрудники.
2. Промышленный шпионаж.
3. Халатность.
4. Низкая квалификация.

И в результате предлагается набор рекомендаций.... без анализа проблемы - **что (кого) и от кого (чего) защищать?** и все ли **механизмы задействованы?**

Структурируем проблему безопасности сетей

Классификация атак

1 По характеру воздействия
2 По цели воздействия
3 По наличию обратной связи с атакуемым объектом
4 По условию начала осуществления воздействия
5 По расположению субъекта атаки относительно атакуемого объекта
6 По уровню эталонной модели ISO/OSI.

По характеру воздействия

- ассивное
- активное

По цели воздействия

- нарушение функционирования системы (доступа к системе)
- нарушение целостности информационных ресурсов (ИР)
- нарушение конфиденциальности ИР
- захват ресурсов

Структурируем проблему безопасности сетей

По наличию обратной связи с атакуемым объектом

- с обратной связью
- без обратной связи (однонаправленная атака)

По условию начала осуществления воздействия

Удалённое воздействие, также как и любое другое, может начать осуществляться только при определённых условиях. Существуют три вида таких условных атак:

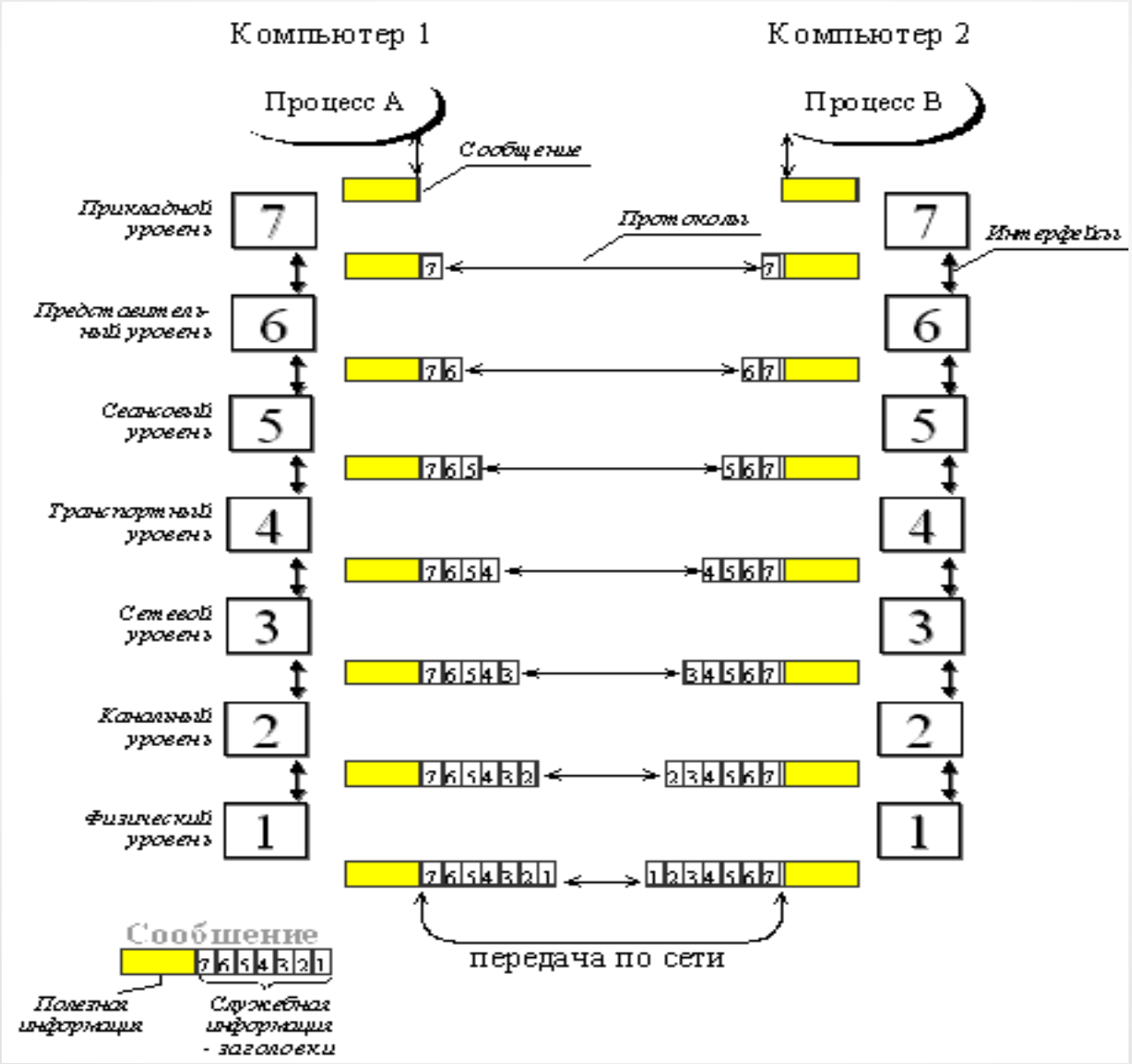
- атака по запросу от атакуемого объекта
- атака по наступлению ожидаемого события на атакуемом объекте
- безусловная атака

По расположению субъекта атаки относительно атакуемого объекта

- межсегментное
- внутрисегментное

По уровню эталонной модели ISO/OSI, на котором осуществляется воздействие

Модель взаимодействия открытых систем ISO/OSI



Структурируем проблему безопасности сетей

Корпоративные (локальные) или глобальные сети ?
(политика безопасности)

По цели воздействия

Что является предметом защиты?
(конфиденциальность, целостность, доступность)

По расположению субъекта атаки относительно атакуемого объекта

Атака изнутри или снаружи?
(близость к защищаемым ресурсам)

По уровню эталонной модели ISO/OSI, на котором осуществляется воздействие

Уровень атаки по модели ISO\OSI?
(атака на приложения, транспорт, сеть и физичесике каналы)

И в результате становится понятным -
что (кого) и от кого (чего) и как защищать?

"Локальные« корпоративные или глобальные сети?

Для корпоративных сетей должна быть определена **политика безопасности.**
То есть определены субъект и объекты и правила доступа, контроль информационных потоков (*что и от кого защищать*).

Такая политика это уровень "приложений" - и если ее нет, то скорее всего вся информация легко доступна!

Как правило для таких сетей атака производится "изнутри"

Если политика есть то возможные цели атаки по всем уровням ISO\OSI сверху вниз, а осуществление атаки происходит снизу вверх!

Для глобальной сети такой общей политики может и не быть (или она не предусматривалась при создании сети) или она чрезвычайно упрощена.

Атака (или ее первый этап), как правило, технически производится "извне"

Атаки носят сложный характер, используя разные уязвимости на разных уровнях модели ISO\OSI

Политики безопасности для корпоративных сетей. Службы каталогов: X.500, DAP, LDAP

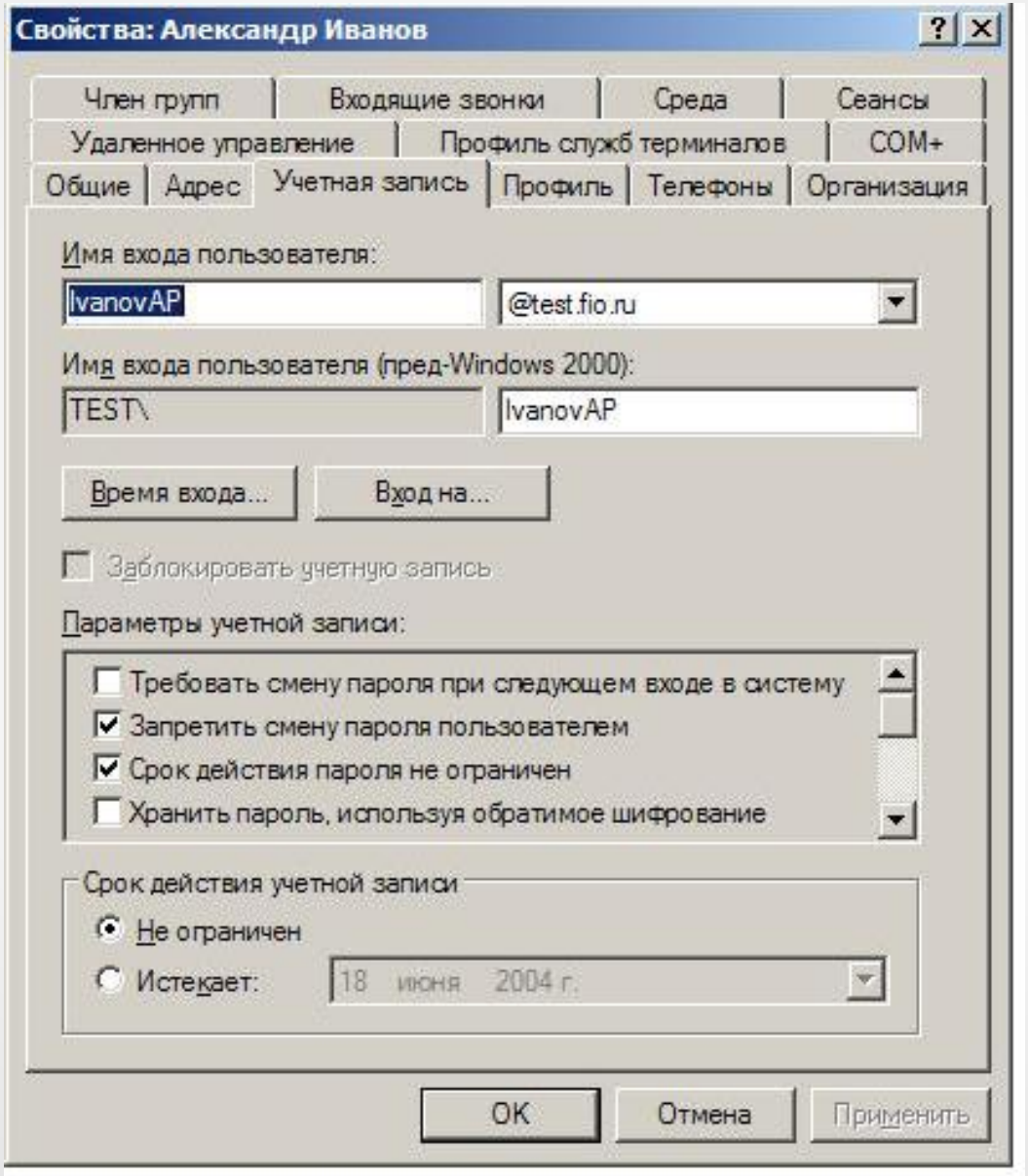
1. **OpenLDAP**
2. ForgeRock OpenDJ
3. Novell eDirectory
4. Apple Open Directory (форк проекта OpenLDAP)
5. **Microsoft Active Directory**
6. **Samba4** LDAP (OpenSource-реализация MS AD)
7. RedHat Directory Server
8. 389 Directory Server (по сути тестовая версия предыдущего)
9. **Oracle Directory Server**
10. Apache Directory Server
11. IBM Tivoli Directory Server
12. **IBM Domino** LDAP
13. CommuniGate LDAP
14. iPlanet Directory

Это инструмент для реализации различных политик безопасности, исползующих **избирательный, мандатный, тематический или ролевой** подход для управления доступом

Основные объекты каталога Active Directory

Значок	Объект	Описание
	Active Directory	Представляет каталог Active Directory в целом. В инструментах управления практически не встречается, за исключением окон поиска и выбора объектов
	Компьютер	Представляет одиночный компьютер в локальной сети. Для компьютеров под управлением Windows NT, 2000 и более поздних версий Windows, является учетной записью компьютера. Объект содержит основные сведения о компьютере и позволяет управлять им
	Домен	Представляет домен Windows. Позволяет управлять параметрами домена
	Контейнер, папка	Представляет простой контейнерный объект. Такие объекты могут создаваться только операционной системой и обычно создаются при установке Active Directory. Похожи на папки файловой системы.
	Пользователь	Представляет учетную запись пользователя.
	Группа	Представляет группу пользователей и обычно используется для упрощения управления
	Контакт	Представляет пользователя — не члена домена. Контакты используются для хранения в каталоге информации о внешних пользователях, не являются учетными записями и не позволяют пользователям регистрироваться в домене
	Принтер	Представляет сетевой принтер. Объект является ссылкой на принтер, предоставленный в общий доступ.
	Общий ресурс	Представляет общую папку. Объект является ссылкой на общий сетевой ресурс и не содержит никаких данных
	Доменная политика	Представляет объект доменной политики. Позволяет настраивать параметры политики уровня домена
	Политика контроллера домена	Представляет объект политики контроллера домена.
	Групповая политика	Представляет объект групповой политики. Позволяет управлять политикой для объектов того контейнера, к которому применена

Основные объекты каталога Active Directory



Основные объекты каталога Active Directory

Типы профилей.
Поддерживаются три типа профилей пользователей:

■Локальный профиль - создается на основе профиля пользователя по умолчанию при первом входе в систему и хранится на локальном компьютере.

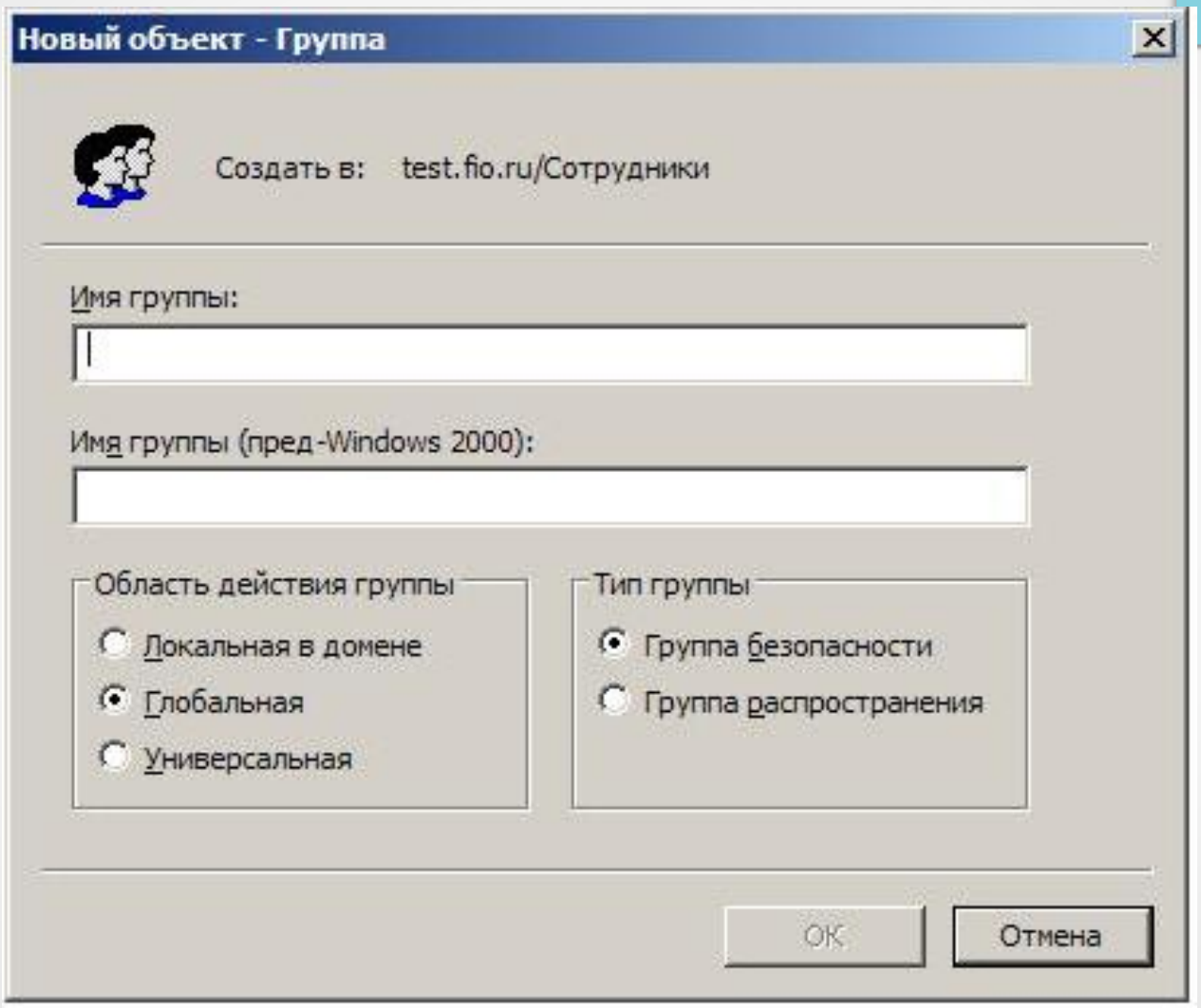
■Перемещаемый профиль - хранится на сервере. При регистрации пользователя на любом компьютере сети перемещаемый профиль копируется на его компьютер. При выходе пользователя профиль копируется обратно на сервер со всеми изменениями, сделанными пользователем.

■Обязательный профиль - хранится на сервере. При регистрации пользователя на любом компьютере сети обязательный профиль копируется на его компьютер. При выходе пользователя профиль не копируется обратно на сервер. В нем не сохраняются изменения пользователя, сделанные во время работы. Профиль всегда постоянен, поэтому может быть связан с несколькими пользователями.

Список основных учетных записей и групп

Имя	Описание
Администратор	Встроенная учетная запись администратора, имеющая неограниченные права
Администраторы	Члены этой группы имеют полные, ничем не ограниченные права доступа к контроллеру домена, любому компьютеру в домене и домену в целом
Администраторы домена	Члены этой группы являются администраторами домена
Гость	Встроенная учетная запись. Используется для регистрации в домене с минимальными правами. После установки эта учетная запись отключена
Гости	Члены этой группы, кроме учетной записи ***Гость***, по умолчанию имеют те же права, что и пользователи
Пользователи домена	Все пользователи домена.
Операторы учета	Члены этой группы имеют права на администрирование учетных записей пользователей и групп в домене
Операторы архива	Члены этой группы могут иметь меньше ограничений только для копирования и восстановления файлов
Операторы печати	Члены этой группы имеют права на администрирование принтеров домена
Операторы сервера	Члены этой группы имеют права на администрирование серверов домена
Имя_контроллера_домена	Учетная запись компьютера - контроллера домена
Владельцы-создатели групповой политики	Члены этой группы могут управлять групповой политикой домена

Список основных учетных записей и групп



Групповые политики

Политики применяются к компьютеру (во время загрузки компьютера) и к пользователю (во время его входа в систему).

Каждая политика определяет соответствующее направление администрирования. Набор параметров политики хранится в Active Directory в контейнере групповой политики.

При инсталляции операционной системы Windows Server устанавливается стандартный набор групповых политик, обеспечивающий безопасность системы.

Контейнер	**Описание**
Сценарии (запуск/завершение)	Содержит параметры *Автозагрузка* и *Завершение работы*, предназначенные для указания файлов сценариев, которые выполняются при загрузке и выключении компьютера
Политика паролей	Содержит параметры, задающие ограничения и правила использования паролей, такие как минимальная длина пароля и срок действия пароля
Политика блокировки учетной записи	Содержит параметры, определяющие правила автоматической блокировки учетных записей при вводе неправильных паролей
Параметры безопасности	Содержит параметры, определяющие поведение системы безопасности, как при локальной работе пользователя, так и при взаимодействии компьютеров в сети
Вход/выход из системы	Содержит параметры, определяющие поведение операционной системы при загрузке компьютера и регистрации пользователя, а также ограничивающие возможности пользователя при выполнении некоторых операций

Управление доступом в Active Directory

По соображениям безопасности администраторы могут использовать управление доступом для контроля доступа пользователей к общим ресурсам.
В Active Directory управление доступом осуществляется на **уровне объектов путем задания для объектов разных уровней доступа** или **разрешений, таких как «Полный доступ», «Запись», «Чтение» или «Нет доступа»**.
Разрешения управления доступом как к общим объектам, так и к объектам Active Directory, хранятся в их дескрипторах безопасности.
В дескрипторе безопасности содержатся две таблицы : избирательная таблица управления доступом (DACL) и системная таблица управления доступом (SACL). По умолчанию объекты Active Directory наследуют права из дескриптора безопасности объекта родительского контейнера.

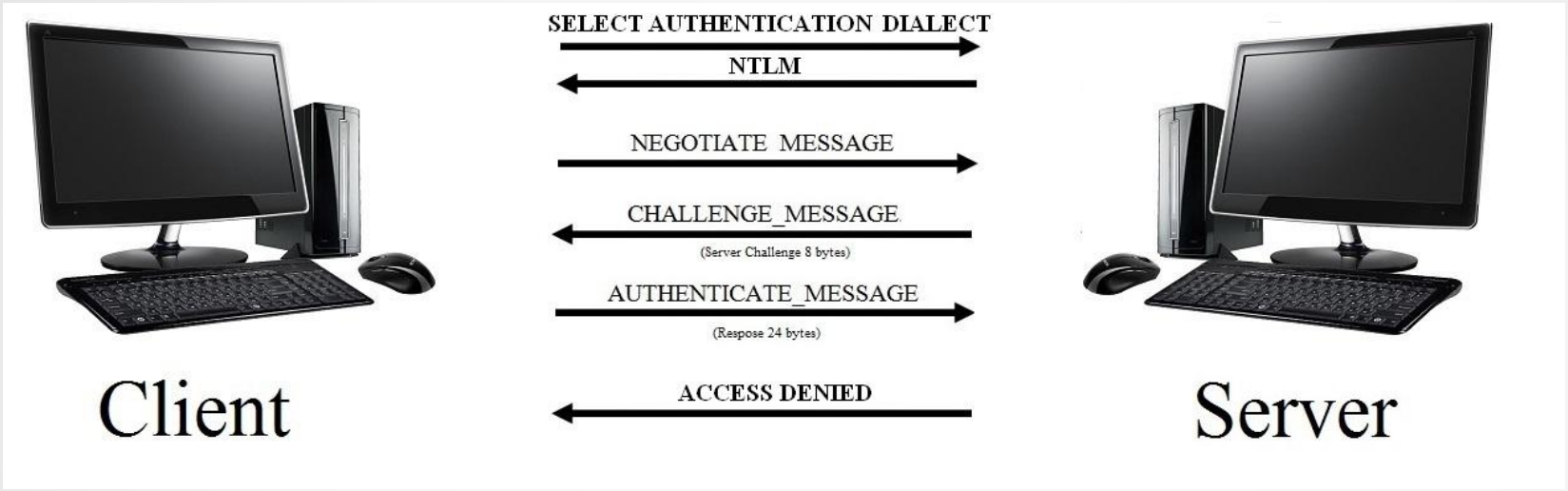
■**Избирательные таблицы управления доступом (DACL).** В DACL указаны пользователи и группы, которым разрешен или запрещен доступ к объекту. Если пользователь или группы, в которые он входит, явно не указаны в DACL, этому пользователю будет запрещен доступ к объекту.

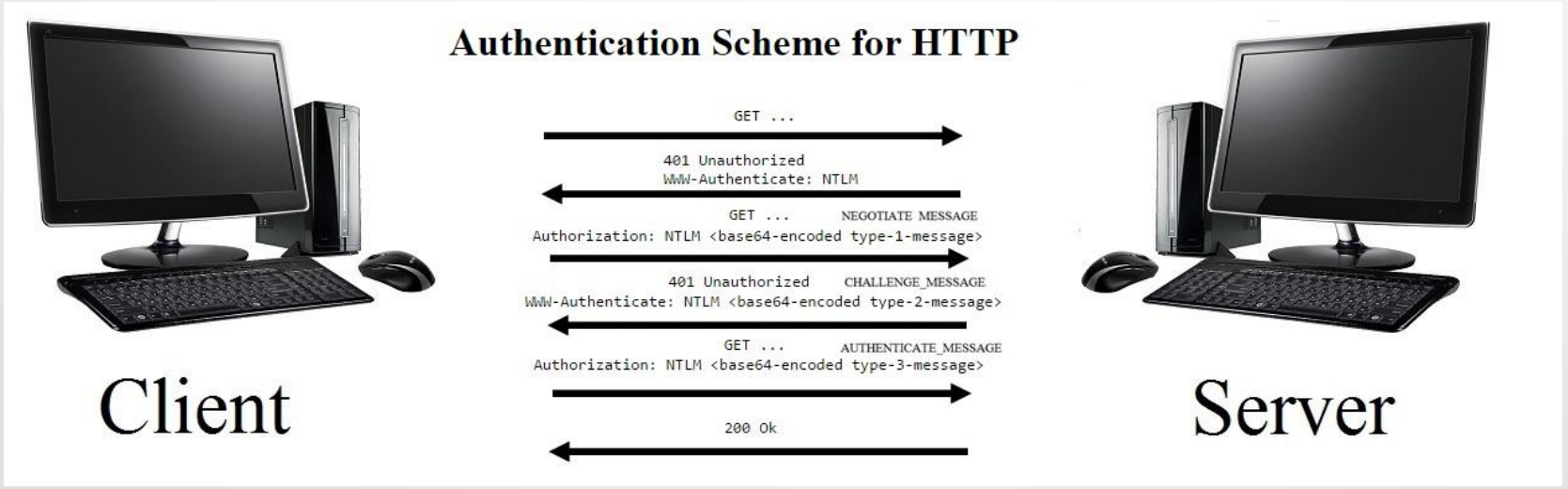
■**Системные таблицы управления доступом (SACL)**. В SACL указаны пользователи и группы, для которых требуется выполнять аудит успешных и безуспешных попыток доступа к объекту.

Идентификация и аутентификация в Active Directory - Kerberos или....

- Клиент, пытается установить соединение с сервером и посылает запрос, в котором информирует сервер, на каких диалектах он способен произвести аутентификации, например: LM, NTLM, NTLM2, NTLMv2. Следовательно, диалект аутентификации LMv2 между клиентом и сервером исключаются.
- Сервер, из полученного от клиента списка диалектов, (по умолчанию) выбирает наиболее защищенный диалект (например NTLMv2), затем отправляет ответ клиенту.
- Клиент, определившись с диалектом аутентификации, пытается получить доступ к серверу и посылает запрос NEGOTIATE_MESSAGE.
- Сервер, получает запрос от клиента и посылает ему ответ CHALLENGE_MESSAGE, в котором, содержится случайная (random) последовательности из 8 байт, она называется Server Challenge.
- Клиент, поучив от сервера последовательность Server Challenge, при помощи своего пароля производит шифрование этой последовательности, а затем посылает серверу ответ AUTHENTICATE_MESSAGE, который содержит 24 байта.
- Сервер, получив ответ, производит туже операцию шифрования последовательности Server Challenge, которую произвел клиент, а затем сравнив свои результаты с ответом от клиента на основании совпадения, разрешает или запрещает доступ.

Идентификация и аутентификация в Active Directory





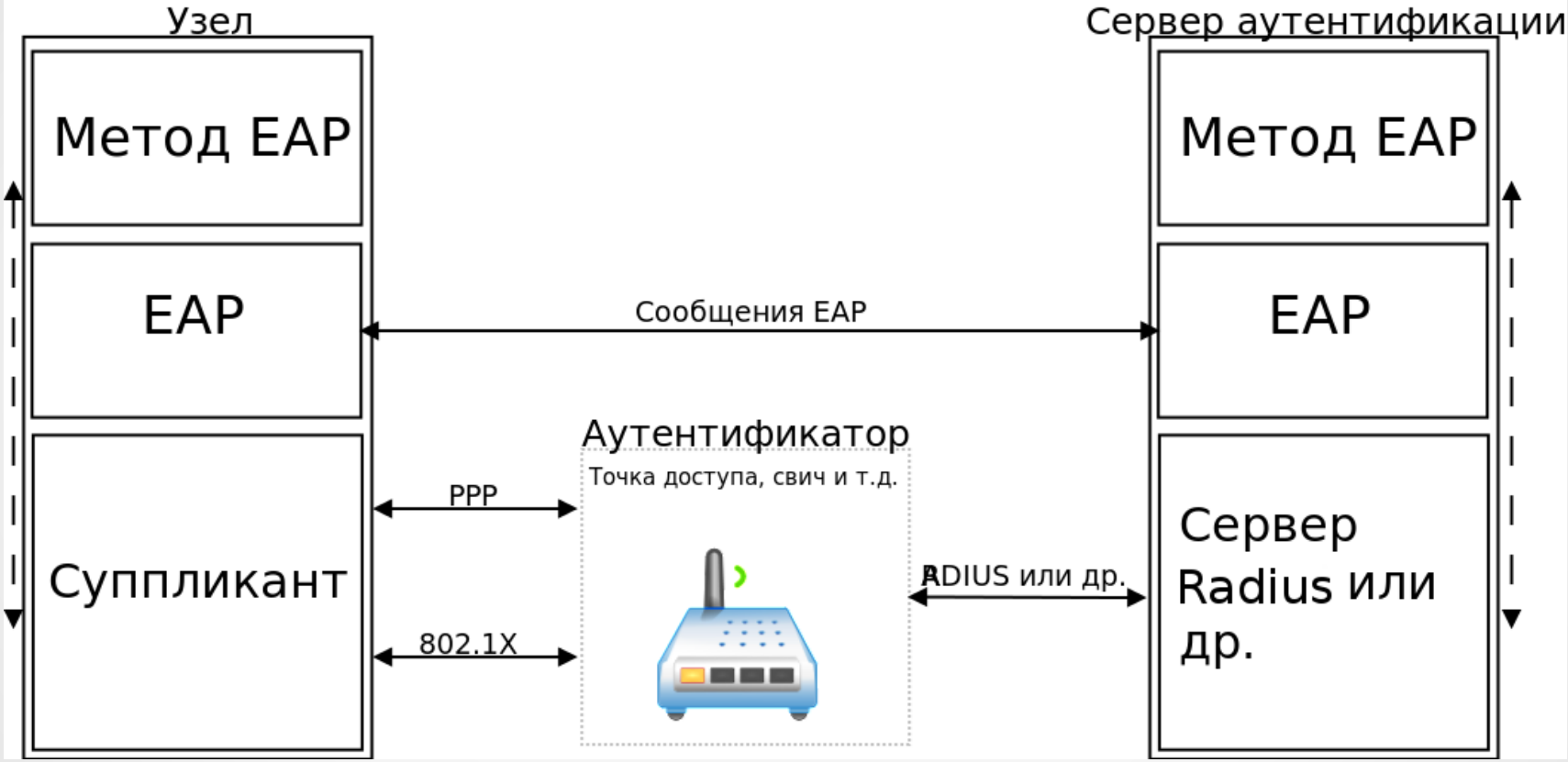
Расширяемый протокол аутентификации EAP в сети.

Известные протоколы: PAP, CHAP, MsCHAP, RADIUS, Kerberos…

EAP (англ. Extensible Authentication Protocol, Расширяемый Протокол Аутентификации) — фреймворк аутентификации, который часто используется в беспроводных сетях и соединениях точка-точка. Формат был впервые описан в RFC 3748 и обновлён в RFC 5247.

В процессе аутентификации можно выделить три основных участника процесса:
Аутентификатор (англ. authenticator) — участник процесса требующий провести аутентификацию (WiFi точка доступа, свитч, сревер и т. д.).
Узел или клиент (англ. peer) — участник процесса который будет аутентифицирован (компьютер, ноутбук, телефон и т. д.).
Сервер аутентификации (англ. authentication server) — участник процесса способный по некоторым данным от узла аутентифицировать его.

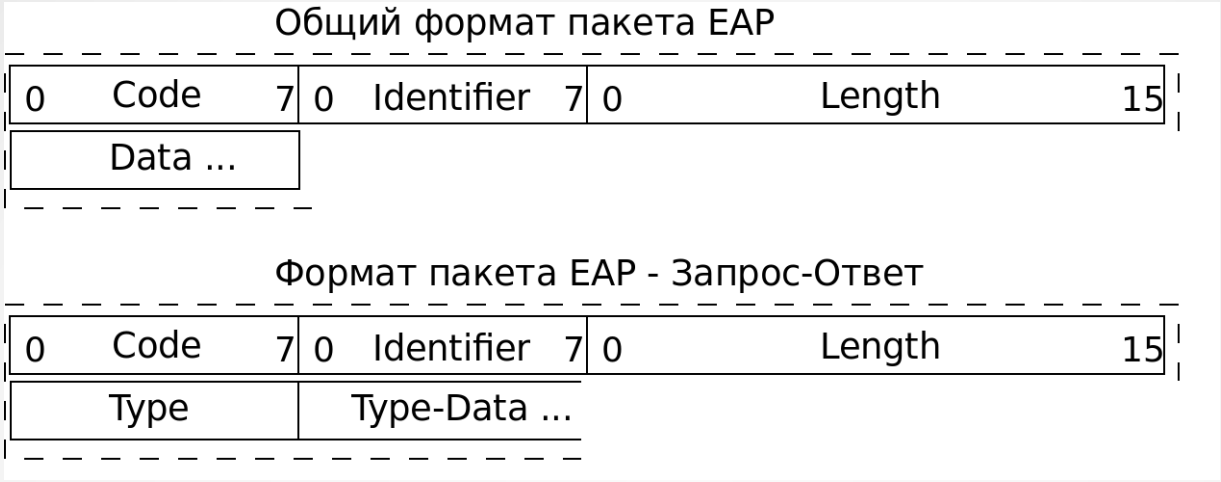
Общая абстрактная схема работы EAP



Общая абстрактная схема работы EAP

1. Аутентификатор отправляет EAP-запрос для начала аутентификации клиента. Запрос в поле Type содержит в себе информацию о том, какой метод будет использоваться (EAP-TLS, EAP-PSK и т. д.).
2. Клиент посылает аутентификатору EAP-ответ в случае правильного запроса от аутентификатора. Ответ содержит в себе поле Type, соответствующее полю Type в запросе.
3. Аутентификатор посылает запрос серверу аутентификации, передавая информацию о том, какой метод аутентификации используется.
4. Сервер аутентификации запрашивает у клиента необходимую информацию через аутентификатор, в этом момент аутентификатор фактически работает как прокси.
5. Клиент отвечает серверу, передавая запрашиваемую информацию. Пункт 4 и 5 повторяются до тех пор, пока сервер аутентификации не примет решение о разрешении доступа, запрете или ошибке.
6. Сервер аутентификации посылает аутентификатору пакет сообщающий о успехе или сбое аутентификации.
7. Аутентификатор посылает клиенту EAP пакет с кодом соответствующим ответу сервера аутентификации (EAP-Success или EAP-Failure).

Общая абстрактная схема работы EAP



CODE:

0 Undefined	Не используется
1 Request	Используется для начала процесса аутентификации аутентификатором, содержит в себе информацию о поддерживаемых методах EAP.
2 Response	Используется для подтверждения начала аутентификации клиентом.
3 Success	Используется для сообщения клиенту о успешной аутентификации.
4 Failure	Используется для сообщения клиенту о провале аутентификации.
5 Initiate	Используется клиентом чтобы «попросить» начать процесс аутентификации.

Поскольку EAP является фреймворком аутентификации, а не конкретным механизмом, он обеспечивает некоторые общие функции и согласование методов проверки подлинности (методы EAP). В настоящее время определенно около 40 различных методов - например: EAP-MD5, EAP-POTP, EAP-GTC, EAP-TLS, EAP-IKEv2, EAP-SIM, EAP-AKA, EAP-AKA‘ и т.д.

Протокол EAP

LEAP - Облегченный расширяемый протокол аутентификации
(англ. Lightweight Extensible Authentication Protocol)

EAP-TLS - Безопасность Транспортного Уровня
(англ. Transport Layer Security)

EAP-TTLS - Tunneled Transport Layer Security
Безопасность Транспортного Уровня через Туннель

EAP-PSK - Pre-Shared Key (Заранее известный ключ),

Общие механизмы защиты сетей

Аутентификация

Дискреционное управление доступом

Мандатное управление доступом

Ролевые и тематические политики доступа

Сегментирование сети (VLAN)

МЭ - фильтрация на уровне сети, сервиса

Proxy, Сетевой периметр, DMZ

Изоляция - криптозащищенные протоколы (PPTP,TLS,IPSec), VPN

VLAN

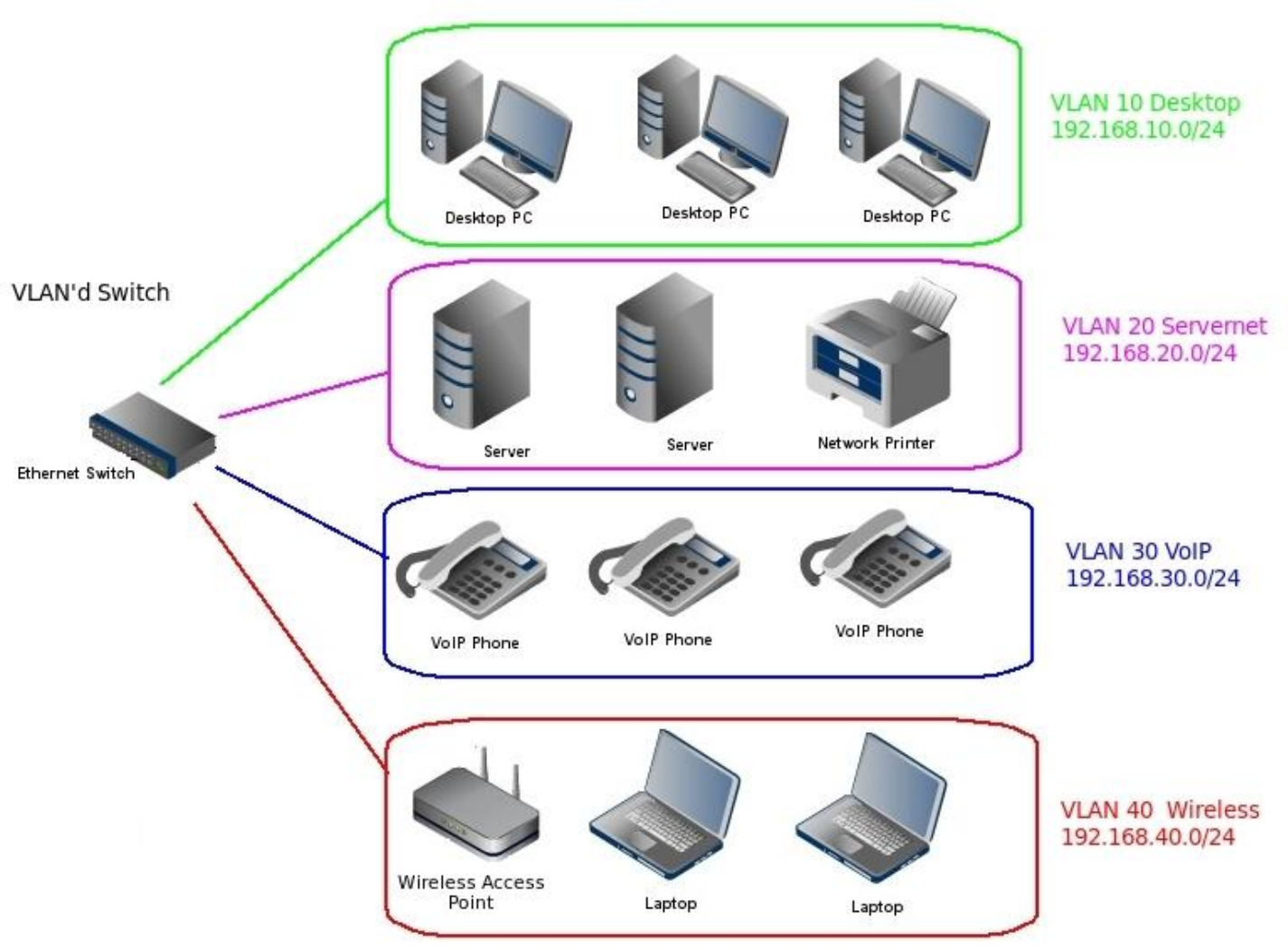
По порту (Port-based, 802.1Q): порту коммутатора вручную назначается одна VLAN. В случае, если одному порту должны соответствовать несколько VLAN (например, если соединение VLAN проходит через несколько свитчей), то этот порт должен быть членом транка. Только одна VLAN может получать все пакеты, не отнесённые ни к одной VLAN (в терминологии 3Com, Planet, D-Link, Zyxel, HP — untagged, в терминологии Cisco — native VLAN). Свитч будет добавлять метки данной VLAN ко всем принятым кадрам не имеющим никаких меток. VLAN, построенные на базе портов, имеют некоторые ограничения.

По MAC-адресу (MAC-based): членство в VLANe основывается на MAC-адресе рабочей станции. В таком случае свитч имеет таблицу MAC-адресов всех устройств вместе с VLANами, к которым они принадлежат.

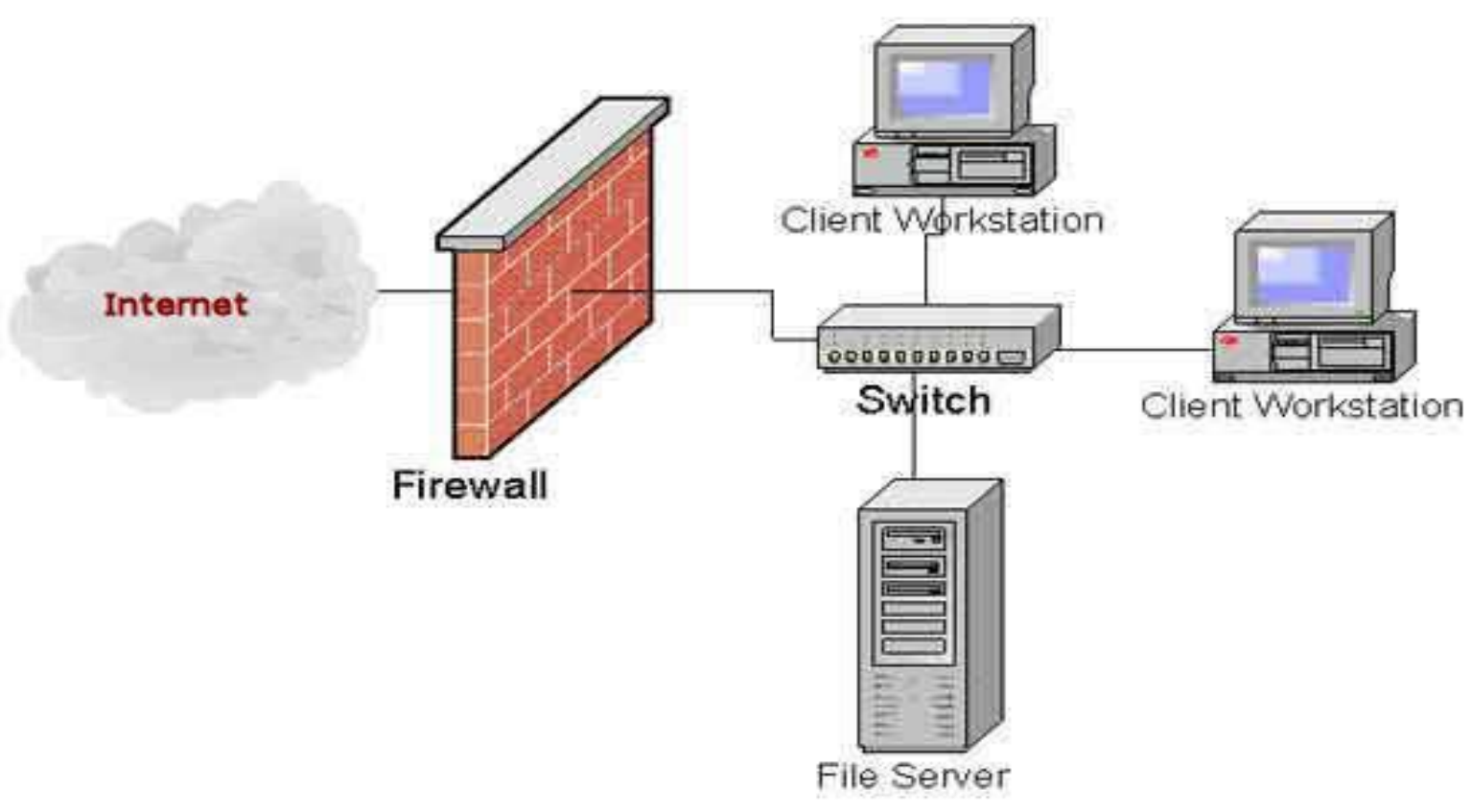
По протоколу (Protocol-based): данные 3-4 уровня в заголовке пакета используются чтобы определить членство в VLANe. Например, IP-машины могут быть переведены в первую VLAN, а AppleTalk-машины во вторую. Основной недостаток этого метода в том, что он нарушает независимость уровней, поэтому, например, переход с IPv4 на IPv6 приведет к нарушению работоспособности сети.

Методом аутентификации (Authentication based): устройства могут быть автоматически перемещены в VLAN основываясь на данных аутентификации пользователя или устройства при использовании протокола 802.1x.

VLAN


VLAN'd Switch
Ethernet Switch
Desktop PC
Desktop PC
Desktop PC
VLAN 10 Desktop
192.168.10.0/24
Server
Server
Network Printer
VLAN 20 Servernet
192.168.20.0/24
VoIP Phone
VoIP Phone
VoIP Phone
VLAN 30 VoIP
192.168.30.0/24
Wireless Access Point
Laptop
Laptop
VLAN 40 Wireless
192.168.40.0/24

Межсетевой экран и периметр сети



Пример фильтрации пакетов

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	Мы им не доверяем
allow	OUR-GW	25	*	*	Подключение к нашему SMTP-порту

Разрешено поступление входящей почты (порт 25 предназначен для входящих сообщений SMTP), но только на компьютер, выполняющий роль шлюза (OUR-GW). Однако поступление почты с внешнего узла SPIGOT блокируется, поскольку этот узел печально известен рассылкой сообщений электронной почты, содержащих очень большие по объему файлы.

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	По умолчанию

Это явное использование политики по умолчанию. Все наборы правил неявно включают это правило в качестве последнего правила.

Общие механизмы защиты сетей

Аутентификация

Дискреционное управление доступом

Мандатное управление доступом

Ролевые и тематические политики доступа

Сегментирование сети (VLAN)

МЭ - фильтрация на уровне сети, сервиса

Proxy, Сетевой периметр, DMZ

Изоляция - криптозащищенные протоколы (PPTP,TLS,IPSec), VPN