

Technischer Überblick für Netzwerkadministratoren

WHITEPAPER

Allgemeines zu diesem Dokument

Dieses Dokument behandelt einige betriebsrelevante und technische Einzelheiten zum NetMotion Mobility XE™ Mobile VPN. Es ist besonders für Netzwerkadministratoren von Nutzen, die besser verstehen müssen, wie Mobility XE funktioniert, bevor sie es in ihrer IT-Umgebung einsetzen. NetMotion Mobility XE und die damit zusammenhängende Technologie ist durch das Urheberrecht und erteilte sowie angemeldete Patente in den USA und anderen Ländern geschützt.

Überblick über die Mobility XE-Architektur

Mobility XE ist ein hochgradig skalierbares, softwarebasiertes mobiles VPN. Es unterstützt sowohl aktive/aktive als auch aktive/passive Hochverfügbarkeit und funktioniert mit einer standardmäßigen Netzwerkinfrastruktur von Routern, Switches und Firewalls. Das Mobility XE-System besteht aus zwei Hauptkomponenten: dem Mobility-Server und dem Mobility-Client. Diese Geräte kommunizieren über Remote Procedure Calls (RPC) und das Internet Mobility-Protokoll (IMP), die auf dem User Datagram-Protokoll (UDP) ausgeführt werden.

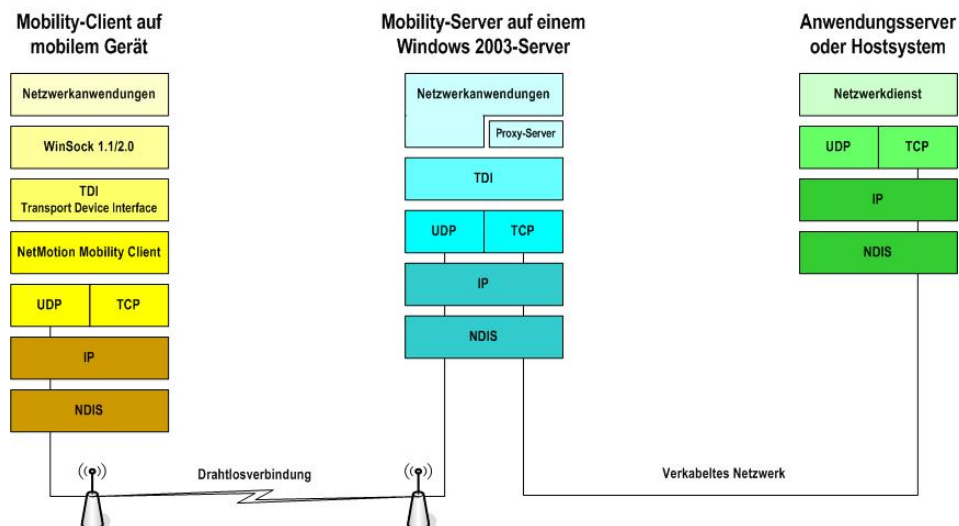
Mobility-Server

Der Mobility-Server verwaltet die drahtlosen Netzwerkverbindungen mobiler Geräte. Er befindet sich im LAN auf einem Computer, auf dem Windows Server 2003 ausgeführt wird.

Der Mobility-Server fungiert als Transportschicht-Proxy für alle mobilen Geräte, auf denen der Mobility-Client ausgeführt wird. Der Server verwaltet den Zustand aller Clients und ist für die komplexe Sitzungsverwaltung zuständig, die zur Aufrechterhaltung kontinuierlicher Verbindungen zu Systemen erforderlich ist, die Netzwerkanwendungen hosten. Wenn ein mobiles Gerät unerreichbar wird, sich im Ruhezustand befindet oder zu einem anderen Netzwerk wechselt, erhält der Mobility-Server die Verbindung zu den Peer-Anwendungen des Clients aufrecht, indem er den Empfang von Daten quittiert und Anfragen in die Warteschlange aufnimmt.

Der Mobility-Server verwaltet darüber hinaus die Netzwerkadressen mobiler Geräte. Jeder Mobility-Client erhält eine virtuelle IP-Adresse im verkabelten Netz. Diese wird in der Regel vom DHCP (Dynamic Host Configuration Protocol) vergeben oder aus einem Adressbereich zugewiesen, der zu diesem Zweck auf dem Mobility-Server reserviert ist. Mobility XE unterstützt darüber hinaus die statische Zuweisung virtueller IP-Adressen an einzelne Geräte oder Benutzer.

Mehrere Mobility-Server können als Server-Pool fungieren und bieten damit Failover und Lastverteilung. In diesem Dokument wird davon ausgegangen, dass die Installation einen einzigen Mobility-Server umfasst. Der Mobility-Server bietet Tools und Statistiken, die der Systemadministrator verwenden kann, um Remote-Verbindungen zu konfigurieren und zu verwalten und Fehler bei diesen Verbindungen zu diagnostizieren. Zur Konfiguration der Mobility XE-Einstellungen und Verwaltung des Servers über einen anderen PC im Netzwerk steht eine webbasierte Schnittstelle zur Verfügung.



Mobility-Client

Die Mobility-Clientsoftware ist bei unterstützten Microsoft-Plattformen auf der TDI-Schicht (Transport Driver Interface) resident und kümmert sich um die Ein- und Umleitung von Anwendungsnetzwerkaufrufen. Wenn eine Anwendung das Netzwerk verwenden möchte, werden die TDI-Aufrufe abgefangen, die Parameter werden aufgestellt und der Aufruf wird zur Ausführung an den Mobility-Server weitergeleitet. Dieser arbeitet transparent mit Betriebssystemfunktionen, damit die clientseitige Anwendungssitzung aktiv bleiben kann, wenn das Gerät den Kontakt mit dem Netzwerk verliert.

Ein Mobility-Clientgerät ist ein standardmäßiges mobiles Gerät oder ein handelsüblicher Computer mit Windows Vista, Windows XP, Windows XP Tablet, Windows Mobile oder Windows CE.

Weitere Infrastruktur

Installationen, die das Analytics Module nutzen, benötigen einen Auswertungsserver und eine Auswertungsdatenbank. Mobility lässt sich auch mit externen Authentifizierungsdiensten integrieren.

Betrieb

Remote Procedure Call- und Internet Mobility-Protokoll

Das Remote Procedure-Protokoll (RPC) und Internet Mobility-Protokoll (IMP) von Mobility XE bilden das technologische Rückgrat, das den Mobility-Server mit den einzelnen mobilen Geräten verbindet.

Ein Remote Procedure Call ist eine Möglichkeit, mit der ein Prozess auf einem lokalen System eine Prozedur auf einem entfernten System aufrufen kann. Bei Mobility XE werden die Netzwerkaufrufe des Clients zur entfernten Ausführung an den Server gesendet. Würde Mobility auf der Winsock-Schicht betrieben, wären dies Aufrufe wie „open socket“, „bind“, „connect“, „send“ und „receive“. Da Mobility XE jedoch auf der TDI-Schicht arbeitet, werden die entsprechenden TDI-Aufrufe zur entfernten Ausführung an den Server weitergeleitet.

Die Anwendung auf dem lokalen System weiß nicht, dass der Procedure Call auf einem entfernten System ausgeführt wird. Der Vorteil des RPC-Ansatzes von Mobility XE liegt darin, dass das mobile Gerät außer Reichweite geraten oder den Betrieb unterbrechen kann, ohne die aktive Netzwerksitzung zu verlieren. Da diese Art der Aufrechterhaltung

von Sitzungen keine anwenderspezifischen Einstellungen und keine Umprogrammierung von Anwendungen erfordert, laufen handelsübliche Anwendungen unverändert in der drahtlosen Umgebung.

Das RPC-Protokoll wird im Internet Mobility-Protokoll (IMP) verkapselt, das wiederum im UDP verkapselt wird. Das Internet Mobility-Protokoll kompensiert die Unterschiede zwischen verkabelten und weniger zuverlässigen Netzwerken durch die Anpassung der Framegrößen und des Protokoll-Timings, um den Netzwerkverkehr zu verringern. Dies wird dann wichtig, wenn eine begrenzte Bandbreite zur Verfügung steht, hohe Latenzzeiten gegeben sind oder der Akku des Mobilgeräts geschont werden soll.

Mobility XE verbessert darüber hinaus die Datensicherheit, indem es den gesamten Datenverkehr zwischen dem Mobility-Server und -Client verschlüsselt und nur authentifizierten Geräten gestattet, eine Verbindung zum Mobility-Server herzustellen. Weitere Informationen zur Sicherheit von Mobility XE finden Sie in *Sicherheit für Drahtlosnetzwerke*.

Registrierung von Geräten

Wenn ein Mobility-Client zum ersten Mal eine Verbindung zum Mobility-Server herstellt, registriert der Server die permanente Gerätekennung oder PID (Permanent Identification) des mobilen Gerätes. Dies ist eine eindeutige Nummer, die der Client für alle nachfolgenden Verbindungen verwendet. Diese Registrierung findet nur bei der ersten Verbindungsaufnahme statt und erfordert keinerlei Eingriff durch den Benutzer oder Administrator. Die Kennung ist in der Registrierung des Client-Systems und im Mobility-Datenspeicher (per LDAP, Lightweight Directory Access Protocol) gespeichert.

Der Mobility-Server speichert die PID basierend auf dem Namen des Computers. Solange sich der Name des Client-Computers nicht ändert, kann der Server die PID auf dem Client-Gerät wiederherstellen, auch wenn die Client-Registrierung verloren geht. Dies kann z. B. passieren, wenn die Festplatte des Client-Geräts neu formatiert und das Betriebssystem neu installiert wird. Wenn der Mobility-Client wieder installiert ist und eine Verbindung herstellt, sucht der Server nach dem passenden Gerätenamen. Wenn dieser gefunden wird, wird dieselbe PID auf dem Gerät wieder hergestellt.

Geräteverbindung

Wenn der Mobility-Client eine Verbindung zum Mobility-Server herstellt, muss der Benutzer sich authentifizieren. Wenn die Authentifizierung erfolgreich ist, erstellen Server und Client einen sicheren VPN-Tunnel, der für die Dauer der Sitzung verwendet wird.

Der mobile Mitarbeiter kann seine regulären Windows-Anmeldeinformationen verwenden, um sich beim Netzwerk zu authentifizieren. Der Mobility-Server authentifiziert den betreffenden Benutzer anhand der Domänendaten des Unternehmens und verwendet hierzu NTLMv2 für die native Microsoft-Authentifizierung, RADIUS-Authentifizierung oder RSA-SecurID-Authentifizierung. Wenn Mobility XE für die RADIUS-Authentifizierung konfiguriert ist, verwendet es das RADIUS-PEAP- oder -EAP-TLS-Protokoll. Dies bietet Unterstützung für eine starke Benutzerauthentifizierung per Public-Key Infrastructure (PKI) unter Verwendung von Chipkarten und/oder Benutzerzertifikaten. (Weitere Informationen hierzu finden Sie weiter unten im Abschnitt „Erweiterte Authentifizierung“.)

Für die Microsoft-Implementierung erfolgt zwischen dem Mobility-Client und -Server ein Dreiwege-Handshake:

- Der Client schickt eine Liste der unterstützten Authentifizierungstypen. Dieses Paket beinhaltet das NTLMv2-Paket HELLO.
- Der Server antwortet mit einer NTLMv2-Challenge.
- Der Client schließt die Authentifizierung mit der Antwort auf die Challenge ab.

Nach der Authentifizierung tauschen Server und Client signierte öffentliche ECC-Schlüssel (Elliptic-Curve Cryptography) und zugehörige kryptografische Daten aus, um einen Diffie-Hellman-Schlüsselaustausch durchzuführen. Symmetrische Schlüssel werden von den öffentlichen Schlüsseln abgeleitet. Diese werden nicht übertragen. Dies gilt für alle unterstützten Authentifizierungsmethoden.

Virtuelle IP-Adressen

Jeder Mobility-Client besitzt eine virtuelle IP-Adresse im verkabelten Netz. Diese wird per DHCP vergeben oder aus einem Adressbereich zugewiesen, der zu diesem Zweck auf dem Mobility-Server reserviert ist. Darüber hinaus können spezifischen Geräten oder Benutzern statische virtuelle IP-Adressen zugewiesen werden. Für jeden aktiven Client leitet der Mobility-Server Daten, die an die virtuelle Adresse des Clients geschickt werden, an die derzeitige tatsächliche Adresse weiter (die so genannte Point-of-Presence- oder POP-Adresse). Während sich die POP-Adresse des Mobility-Clients ändert, wenn das Gerät von einem Funkbereich in einen anderen wechselt, bleibt die virtuelle Adresse die gesamte Sitzung über gleich.

Sitzungspersistenz

Im Gegensatz zu IPsec- oder SSL-VPN erfordert das Mobility XE-VPN keine feste lokale Adresse. Der Tunnel zwischen dem Mobility-Server, der eine feste Adresse hat, und dem Mobility-Client, dessen POP-Adresse sich ständig ändern kann, wird aufrechterhalten. In gegenseitigem Übereinkommen halten Client und Server einen sicheren Tunnel offen, bis einer der Endpunkte einen Trennungsbefehl ausgibt. Dies kann geschehen, wenn der Benutzer sich abmeldet, der Administrator das Gerät unter Quarantäne stellt oder die konfigurierbare Inaktivitätszeit überschritten wird.

Der Tunnel bleibt verfügbar und Anwendungssitzungen werden unter unterschiedlichsten Umständen aufrechterhalten:

- Aktivieren und späteres Deaktivieren des Ruhezustands beim mobilen Gerät
- Ortswechsel im Netz
- Verbindung eines mobilen Geräts über ein langsames Netzwerk mit beschränkter Bandbreite oder hoher Latenzzeit
- Störung durch Mikrowellen, Treppenhäuser, Aufzugsschächte oder andere Hindernisse, die Funksignale stören
- Wechsel der Netzwerkschnittstelle (z. B. von WLAN- zu WWAN-Karte)
- Funklöcher

Das konfigurierbare Zeitlimit gewährleistet, dass die auf dem Mobilitäts-Server durch inaktive Sitzungen belegten Ressourcen nicht auf unbegrenzte Zeit belegt bleiben. In Testszenarien wurden Geräte jedoch mitten in einer Anwendungstransaktion in den Standbymodus versetzt und eine Woche später aufgeweckt und die Transaktion ging an genau der Stelle weiter, an der sie unterbrochen worden war.

Anwendungspersistenz

Netzwerkanwendungen sind so geschrieben, dass sie Schnittstellen auf Anwendungsebene nutzen können, wie z. B. Winsock (die Windows Sockets-API). Ein

einzigem Aufruf an die API auf Anwendungsebene kann mehrere ausgehende oder eingehende Datenpakete auf der Transportschicht (IP) erzeugen. Wenn in bestehenden mobilen Netzwerken eines dieser Pakete verloren geht, kann die gesamte Verbindung in einen unklaren Zustand übergehen und die Sitzung zusammenbrechen.

Das Internet-Mobility-Protokoll (IMP) überwindet diese Probleme. Das Protokoll emuliert das Verhalten einer verkabelten Verbindung, sorgt für die zuverlässige Weiterleitung von Daten und bewältigt verschiedene Situationen, darunter Netzwerkwechsel und Verbindungsunterbrechungen während einer Übertragung. Die logische Sitzung wird aufrechterhalten und bleibt auch dann offen, wenn das Gerät unerreichbar ist oder in den Standbymodus versetzt wird.

Vom Standpunkt der Anwendung auf dem mobilen Gerät aus gesehen wartet die Anwendung einfach, bis sie eine Antwort erhält, es sei denn, es kommt zu einer Zeitüberschreitung. Mobility XE erzielt dieses Verhalten, wenn der Server unerreichbar ist, indem die Operation in einen Wartezustand versetzt wird. Die Winsock-Schnittstelle gibt dann der Anwendung die richtige Antwort zurück, gleichgültig ob sie Blocking Calls, Asynchronous Calls oder überlappende I/O verwendet. Die Anwendung sieht dieselben Antworten und dasselbe Verhalten wie in einem verkabelten Netzwerk.

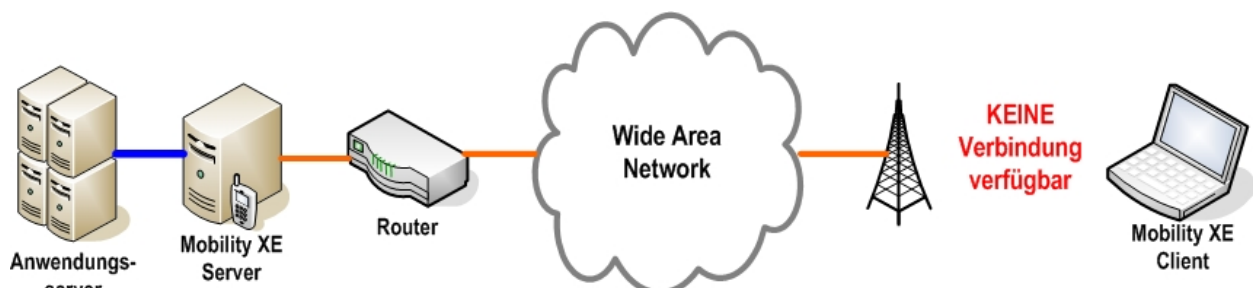
Verwalten des Verbindungszustands

Mobility XE führt keinen „Test“ durch, um festzustellen, ob das Gerät erreichbar ist, bevor Daten gesendet werden – es überträgt einfach die erforderlichen Daten und wartet auf die Quittierung. Wenn die Quittierung nicht eintrifft, wird die Übertragung einige Male wiederholt. Mobility XE stellt dann die Übertragung ein, stellt fest, dass das Gerät nicht erreichbar ist und sendet die Daten später erneut. Das Statusmodul des IMP verfolgt gesendete Pakete, quittierte Pakete und Pakete, die neu gesendet werden müssen, und hält damit die Integrität der gesamten Sitzung aufrecht.

Um zu bestimmen, ob ein inaktives mobiles Gerät erreichbar ist, verwendet das Mobility XE-System Keep-Alives: Der Mobility-Client versendet in regelmäßigen Abständen Frames an den Mobility-Server. Die Häufigkeit dieser Keep-Alive-Frames ist vom Benutzer konfigurierbar und kann reduziert werden, um den Verkehr bei Netzwerken mit beschränkter Bandbreite zu verringern. Wenn der Mobility-Server die erwarteten Keep-Alive-Frames nicht innerhalb des vorgegebenen Zeitraums empfängt, zeigt die Verwaltungskonsole des Servers, dass das Gerät nicht erreichbar ist. Keep-Alives werden nur verwendet, wenn kein Anwendungs- oder sonstiger Datenverkehr stattfindet.

Das Gerät ist nicht erreichbar

Weil Mobility XE mit RPC arbeitet, wird der Zustand unterbrochener Datenübertragungen aufrecht erhalten und die Daten bleiben in der Warteschlange.



Mobility XE sorgt dafür, dass der VPN-Tunnel sowie Anwendungen und Daten erhalten bleiben, wenn der Client nicht erreichbar ist.

Wenn der Anwendungsserver Daten an den Mobility-Client überträgt und der Client aufgrund einer Netzwerkunterbrechung oder die Versetzung des Geräts in den Standby-Zustand unerreichbar wird, weisen die Datenflusskontrollalgorithmen von Mobility XE die RPC-Schicht des Mobility-Servers an, keine Daten mehr vom Anwendungsserver anzunehmen. Die TCP-Puffer des Mobility-Servers füllen sich und das TCP-Fenster wird infolgedessen auf Null (0) eingestellt. Dadurch wird wiederum der Anwendungsserver informiert, dass die Datenübertragung unterbrochen werden muss, bis der Mobility-Client in der Lage ist, Daten zu empfangen. In diesem Zustand tauschen der Mobility-Server und der Anwendungsserver TCP-Quittungen aus, um die Verbindung auf unbestimmte Zeit oder solange wie vom Administrator konfiguriert offen zu halten.

Wenn der Client wieder erreichbar ist, empfängt die RPC-Schicht eine Flusskontrollanweisung, die angibt, dass die Datenübertragung fortgesetzt werden kann. Die RPC-Schicht nimmt dann den Datenempfang vom TCP-Stack wieder auf, wodurch sich die Empfangspuffer der TCP-Verbindung wieder leeren. Wenn wieder Speicherplatz verfügbar wird, stellt der TCP-Stack das Empfangsfenster der Verbindung auf einen anderen Wert als Null ein, was dem TCP-Stack des Anwendungsservers angibt, dass wieder Daten empfangen werden können. Die Datenübertragung wird wieder aufgenommen.

Das Gerät ist in ein anderes Netzwerk gewechselt

Mobility XE nutzt DHCP, um das so genannte „Roaming“ zu erkennen und zu ermöglichen, d. h. wenn das mobile Gerät eine Subnetzgrenze überschreitet oder in ein anderes Netzwerk wechselt. Der Benutzer muss das System nicht neu starten oder bestehende Netzwerkverbindungen schließen, um eine neue Adresse zu erhalten.

Subnetz-Roaming

Mit Mobility XE können mobile Geräte Subnetzgrenzen überschreiten, ohne dass ihre Netzwerkverbindung oder die Anwendungssitzung verloren geht. Hierzu muss der Mobility-Client erkennen können, dass er sich in einem neuen Subnetz befindet, und eine neue POP-Adresse vom DHCP-Server anfordern können.

Der Mobility-Client verwendet zwei Methoden, um zu erkennen, dass er sich in einem neuen Subnetz befindet. Eine Methode basiert auf Informationen vom Netzwerkkartentreiber. Dies ist die bevorzugte Methode. Die andere Methode basiert auf DHCP-Beaconing und erfordert einen regelmäßigen DHCP-Discover/Offer-Austausch. Beide Methoden für das Subnetz-Roaming nutzen zumindest teilweise DHCP-Dienste, um Roaming zu ermöglichen. Der Mobility-Client verwendet DHCP-Dienste, um seine IP-Adresse und andere optionale Konfigurationsparameter für das neue Netzwerk oder Subnetz zu ermitteln.

Roaming-Erkennung in drahtlosen WANs

In einem WWAN kümmert sich die Netzwerkinfrastruktur um das Roaming. Beaconing ist hier nicht erforderlich. Das Beaconing wird automatisch deaktiviert, wenn eine der folgenden Bedingungen zutrifft:

- Der Mobility-Client ist über eine Wählverbindung oder einen PPP-Netzwerkadapter (Point-to-Point-Protokoll) verbunden.
- Der Netzwerkadapter des Mobility-Clients erhält eine statische IP-Adresse und muss die IP-Adresse nicht ändern, um im drahtlosen WAN zu roamen (d. h. das Roaming ist in der dem WWAN zu Grunde liegenden Infrastruktur aktiviert).

Roaming-Erkennung in einem Supernet-Netzwerk

Mobility XE bietet eine Einstellung, die die beacon-basierte Roaming-Erkennung in einem Supernet-Netzwerk verändert. Dabei handelt es sich um ein Netzwerk, in dem zwei Bedingungen gegeben sind:

- Ein einzelnes physisches Netzwerk unterstützt zwei oder mehr logische Netzwerke.
- DHCP-Server weisen Mobility-Clients IP-Adressen in mehr als einem logischen Netzwerk zu.

Wenn beide Bedingungen zutreffen und die Netzwerkumgebung nicht leicht modifiziert werden kann, um die IP-Adresszuweisung für Mobility-Clients zu erleichtern, kann die Performance des beacon-basierten Roamings durch die Aktivierung des Supernet-Roaming auf dem Mobility-Server verbessert werden, weil damit häufige unnötige Roaming-Versuche verhindert werden.

InterNetwork Roaming™

Ein Mobility-Client kann beim Wechsel zwischen verschiedenen Netzwerkmedien Verbindungen und Anwendungssitzungen aufrecht erhalten. Wenn in dem mobilen Gerät Netzwerkkarten für unterschiedliche Netzwerkverbindungsarten installiert und richtig konfiguriert wurden, ermöglicht Mobility XE die Persistenz von Anwendungen, wenn der Client zwischen einem LAN, einem WLAN, einem WWAN und allen anderen Arten von IP-basierten Netzwerken wechselt. Auf dem Mobility-Client und -Server sind keine weiteren Konfigurationen erforderlich.

Das Betriebssystem und die Netzwerkhardware des mobilen Geräts bestimmen, wie viel Benutzereingriff für InterNetwork Roaming™ erforderlich ist. Ein Mobility-Client mit mehreren aktiven Netzwerkschnittstellen kann möglicherweise automatisch von einer Schnittstelle zur anderen wechseln. Wenn sich beispielsweise ein Client-Gerät mit WLAN- und WWAN-Karte aus dem Bereich eines WLAN-Zugangspunkts entfernt, kann die Kommunikation automatisch auf das WWAN-Medium umgestellt werden.

Bei einem Client-Gerät, bei dem gleichzeitig mehrere Netzwerkkarten aktiv sind, verwendet Mobility XE die Schnittstelle, die das Betriebssystem verwendet. Die Schnittstellenwahl des Betriebssystems hängt möglicherweise von der Reihenfolge ab, in der die Schnittstellen aktiviert werden, wodurch möglicherweise nicht immer die „beste“ Schnittstelle verwendet wird. Der Mobility-Server ändert die Parameter für eine definierte Route im Client-Betriebssystem je nach Geschwindigkeit der Netzwerkschnittstelle, damit das mobile Gerät die verfügbare Schnittstelle mit der größeren Bandbreite verwendet. Wenn die Option „Roaming – Schnellste Schnittstelle verwenden“ deaktiviert ist, muss der Benutzer je nach Betriebssystem möglicherweise Schnittstellenkarten manuell deaktivieren und aktivieren.

Manchmal können Netzwerkverbindungen über zwei Schnittstellen hergestellt werden, der Mobility-Server ist jedoch nur über eines dieser Netzwerke erreichbar. Durch die Client-Netzwerk-Failover-Funktion von Mobility XE kann sich der Client auch dann verbinden, wenn die bevorzugte Schnittstelle vorhanden ist, jedoch keine Verbindungsmöglichkeit zu einem Mobility-Server bietet. Detaillierte Informationen zu Roaming-Erkennung und -Verhalten finden Sie im Systemadministratorhandbuch zu Mobility XE.

NAT (Network Address Translation)

Da Mobility UDP verwendet, ist es nicht für die typischen Probleme anfällig, die bei IPSec-VPN und NAT auftreten. IPSec-VPN sind gezwungen, NAT-T (NAT Traversal, siehe RFC 3947) anzuwenden, wobei IPSec-ESP-Pakete in UDP verkapselt werden, um Firewalls und Router zu passieren, die NAT nicht unterstützen. Da Mobility XE konzeptbedingt NAT unterstützt, sind diese zusätzliche Verkapselung und der Daten-Overhead zum Passieren der Knoten zwischen dem Mobility-Client- und -Server überflüssig.

Erweiterte Authentifizierung

Mobility XE unterstützt mehrere verschiedene Zwei-Faktor-Authentifizierungsmethoden. Neben einem Benutzernamen und einem Passwort oder einer PIN (etwas, das der Benutzer kennt) ist bei der Zwei-Faktor-Authentifizierung auch noch etwas erforderlich, das der Benutzer besitzt (z. B. ein Zertifikat, ein Schlüsselanhänger usw.). Es werden dabei folgende Methoden unterstützt:

- Sicherheits-Token (z. B. ein RSA® SecurID-Schlüsselanhänger)
- Chipkarten (die von einem Kartenleser gelesen werden), einschließlich solcher, die mithilfe eines Biometricscanners den Fingerabdruck eines Benutzers erkennen, der dann anstelle einer PIN oder eines Passworts zugelassen wird
- Benutzerzertifikate, die auf der Gerätefestplatte gespeichert sind

RSA SecurID

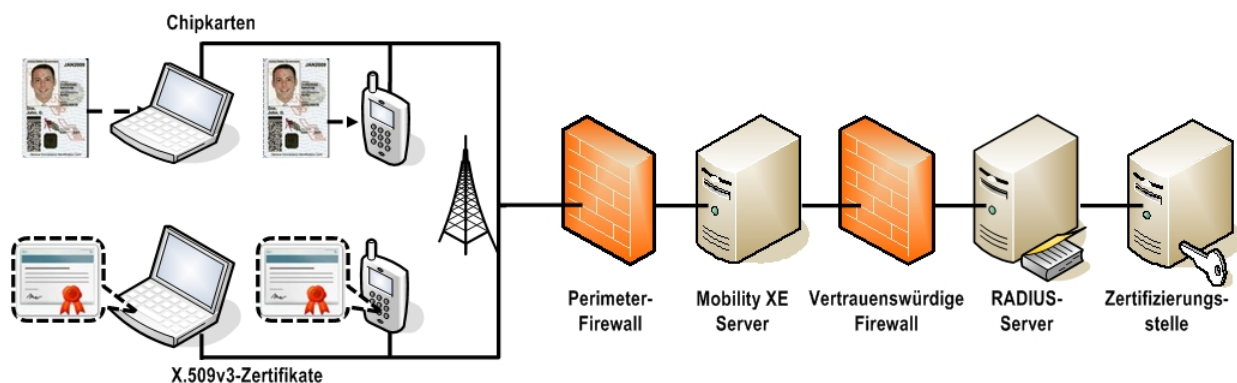
RSA SecurID authentifiziert Benutzer anhand ihrer Fähigkeit, nach der Eingabe ihrer persönlichen Identifikationsnummer (PIN) eine sich häufig ändernde Zeichenfolge aus Ziffern und Buchstaben einzugeben, die durch einen Token-Generator erzeugt wird. Bei diesem Token-Generator kann es sich um einen Hardware-Generator handeln, beispielsweise einen Schlüsselanhänger oder einen USB-Token, der einen zeitbasierten Code anzeigt, der vom Benutzer manuell eingegeben werden muss. Es kann sich aber auch um eine Software-Anwendung handeln, die auf dem Gerät des Benutzers ausgeführt wird und die Zeichenfolge ausgibt.

Bei einer RSA-SecurID-Installation wird die Software RSA Authentication Agent auf dem Mobility-Server ausgeführt. Diese verschlüsselt die eingegebenen Anmeldedaten mit einem Einweg-Hash und gibt sie anschließend an den RSA Authentication Manager weiter, der auf einem anderen Server ausgeführt wird. Der RSA Authentication Manager überprüft die Anmeldedaten und gibt den Authentifizierungsstatus an den Mobility-Server zurück. Mobility XE unterstützt auch die Verfahren, in regelmäßigen Abständen eine neue SecurID-PIN für die Bereitstellung neuer Tokens zu generieren (New PIN Mode) und mehrere aufeinanderfolgende Tokencodes einzugeben (Next Token Mode). Mobility XE hat das *RSA Secured* Partner Program-Zertifikat für das RSA-SecurID-Produkt erhalten. Dieses Zertifizierung bedeutet, dass eine technische Partnerschaft besteht, um die Sicherheit für gemeinsame Kunden zu erhöhen, die beide Produkte verwenden.

PKI/RADIUS

Mobility XE unterstützt standardkonforme Zwei-Faktor-Authentifizierungslösungen, die digitale Zertifikate nutzen und zu deren Validierung die Authentifizierung per PKI (Public Key Infrastructure) und RADIUS Extensible Authentication Protocol (EAP) einsetzen. Bei der RADIUS-EAP-Implementierung von Mobility XE handelt es sich um eine weithin verwendete Ausführung des Sicherheitsstandards 802.1x. Die PKI-Technologie ist in

den Betriebssystemen von Microsoft und in zahlreichen Lösungen von anderen Herstellern integriert und unterstützt den international gültigen Standard X.509v3 für digitale Zertifikate.



Starke Authentifizierung unter Nutzung von RADIUS und PKI-validierten Zertifikaten

Damit die Anforderungen der PKI-basierten Authentifizierung erfüllt werden, müssen auf den Mobility-Clients und RADIUS-Servern Zertifikate für die gegenseitige Authentifizierung installiert sein. Auf dem RADIUS-Server muss Folgendes installiert und konfiguriert sein:

- Digitales X.509v3-Zertifikat und privater Schlüssel
- Zertifikat für die vertrauenswürdige Zertifizierungsstelle (CA), die die Zertifikate auf den Client-Geräten signiert hat

Auf den Mobility-Clients muss Folgendes installiert und konfiguriert sein:

- Zertifikat für die vertrauenswürdige Zertifizierungsstelle (CA), die das Zertifikat auf dem RADIUS-Server signiert hat
- Das X.509v3-Zertifikat muss installiert und konfiguriert sein oder es muss eine Chipkarte mit einem gültigen, von der Zertifizierungsstelle des Unternehmens herausgegebenen Zertifikat zur Verfügung stehen
- Bei Verwendung von Chipkarten ein Lesegerät, das Microsoft CSP (Cryptographic Service Provider) unterstützt

Der Mobility-Server agiert im RADIUS-Sicherheitssystem als Network Access Server (NAS). Das Authentifizierungsprotokoll EAP-TLS wird vom Client über den RADIUS-Server an den Authentifizierungsserver weitergegeben. Wenn der Client mit passwortgeschützten digitalen Zertifikaten arbeitet, die auf seiner Festplatte gespeichert sind, muss der Benutzer das Zertifikatpasswort eingeben, um die Zertifikate zu entsperren. Ist das Zertifikat auf einer Chipkarte gespeichert, muss der Benutzer die entsprechende PIN eingeben. Der Mobility-Server und der Mobility-Client bauen anschließend einen gegenseitig authentifizierten, sicheren Tunnel auf, der durch die x.509-Zertifikate geschützt ist.

Der Mobility-Server gibt die Benutzeranmeldedaten an den RADIUS-Server weiter. Der RADIUS-Server führt die Authentifizierung durch, indem er das Zertifikat anhand der Zertifizierungsstelle validiert. Falls der RADIUS-Server die Anmeldedaten erfolgreich authentifiziert, benachrichtigt er den Mobility-Server, der daraufhin den Benutzerzugriff auf die Mobility XE Services gestattet. Falls der RADIUS-Server das Zertifikat nicht

authentifizieren kann, lehnt er die Authentifizierungsanforderung ab und der Mobility-Server bricht den Verbindungsversuch ab.

Die Methode der Zwei-Faktor-Authentifizierung unterstützt Biometriesysteme wie Fingerabdruckscanner, wenn diese Systeme anstelle eines Passworts zum Entsperren des Zugriffs auf gespeicherte Zertifikate verwendet werden. Genaue Anweisungen zur Konfiguration der gängigsten RADIUS-Server finden Sie im Systemadministratorhandbuch zu Mobility XE.

Verbindungsoptimierung

Zahlreiche seiner Verhaltensweisen schränken den Nutzen des Protokolls TCP/IP für drahtlose Umgebungen stark ein. Zur Behebung dieser Schwachpunkte ist Mobility XE so konzipiert, dass auch bei instabilen und langsamen Netzwerkverbindungen eine optimale Leistung erzielt werden kann. Seine Architektur umfasst Verbesserungen, die dem IP-basierten Netzwerkverkehr eine effektivere Handhabung kurzfristiger Verbindungsunterbrechungen ermöglichen, wie sie bei mobilen Geräten durch Funklöcher oder sonstige Faktoren wie Energiesparmodi und Benutzereingriffe auftreten können. Es gestattet eine höchst effiziente Ausnutzung der vorhandenen Bandbreite und setzt zahlreiche fortschrittliche Funktionen zur Verringerung des Overheads von Transportprotokollen ein:

- Selektive Bestätigung
- Daten- und Bestätigungsbündelung
- Nachrichtenverschmelzung
- Verringerte und synchronisierte Neuübertragungen
- Fragmentierungsoptimierung
- Datenkomprimierung
- Fehlerverringerungs-Algorithmen
- Web-Beschleunigung

In Kombination ermöglichen diese erweiterten Funktionen eine maximale Effizienz bei dem Datentransport. Wenn die Option „Use Fastest Interface“ (Schnellste Schnittstelle verwenden) aktiviert ist (Standard), schaltet Mobility XE außerdem automatisch zur schnellsten Netzwerkverbindung um, falls mehrere Verbindungen aktiv sind.

Nachstehend finden Sie Beschreibungen dazu, wie diese Funktionen im Einzelnen die drahtlose Übertragung unterstützen, insbesondere in WWANs.

Algorithmus für selektive Bestätigungen

Bei der Übertragung von Daten über eine WWAN-Verbindung kann der Verlust von Paketen einen schwerwiegenden Einfluss auf die Leistung haben. Wenn eine der Seiten eine Folge von Paketen überträgt, ist es gut möglich, dass einige der Frames unterwegs verloren gehen und nie ihr endgültiges Ziel erreichen.

Mobility XE berücksichtigt beim Senden und Empfangen von Daten mögliche Paketverluste. Durch die Verwendung von laufenden Nummern kann Mobility feststellen, ob ein Frame in falscher Reihenfolge empfangen wurde. Wenn es einen Frame empfängt, der eine höhere Nummer trägt als erwartet, wird das übertragende Gerät benachrichtigt, dass einer oder mehrere Frames nicht angekommen sind. Daraufhin überträgt das übertragende Gerät die fehlenden Frames erneut.

Im Gegensatz dazu übertragen Implementierungen ohne selektive Bestätigung nicht nur die fehlenden Frames, sondern ggf. auch die Frames, die ordnungsgemäß

angekommen sind. Diese überflüssigen Neuübertragungen verschwenden Bandbreite und die Verarbeitungsressourcen.

Nachrichtenverschmelzung, Daten- und Bestätigungsbündelung

Die meisten Standardimplementierungen von Netzwerkprotokollen nutzen Bestätigungs-Frames, um dem sendenden Gerät zu bestätigen, dass die gesendeten Pakete erfolgreich beim empfangenden Gerät angekommen sind. Dabei handelt es sich um eine fortlaufende Rückmeldung: Im besten Fall wird jeder zweite Frame bestätigt, was einen Datenstrom von kleinen Kontroll-Frames Gegenrichtung erzeugt. Diese zusätzlichen Frames sind zwar klein, können sich aber zu einem erheblichen Overhead aufaddieren.

Mobility XE kann den Rückfluss von Daten von jedem zweiten Frame auf jeden vierten Frame (oder noch mehr) reduzieren. Dies wird durch Einsatz der Richtlinie für die selektive Bestätigung und durch Anpassung der Parameter zur Ermittlung der Netzwerklatenz erreicht. Dadurch können mehr Daten auf Anwendungsebene übertragen werden, weil weniger Bandbreite für zusätzliche Kontrolldaten erforderlich ist.

Zur weiteren Verringerung der Bandbreitennutzung arbeitet Mobility XE mit Nachrichtenbündelung (bzw. Multiplexing). Mithilfe dieses Algorithmus lassen sich Kontroll- und Anwendungsdaten aus mehreren verschiedenen Nachrichtenströmen gemeinsam innerhalb desselben Frames übertragen. Ohne diese Funktion werden die Daten in eigene Frames verkapselt, wenn sie von einer Anwendung übertragen werden. Bei mehreren Verbindungen erhöht sich entsprechend der Protokoll-Overhead. Durch die Bündelung dieser Datenströme ermöglicht Mobility, dass mehr Daten auf demselben Raum übertragen werden können, was zu einer deutlich besseren Nutzung der Bandbreite führt.

Ein weiterer Vorteil dieser Methode besteht darin, dass die Kapazität jedes Frames maximal ausgenutzt werden kann. Im folgenden Beispiel senden und empfangen zwei Anwendungen Daten in einer herkömmlichen Implementierung: Anwendung A sendet 100 Byte Daten an ihre Gegenstelle und Anwendung B sendet 150 Byte an ihre Gegenstelle.

Bei einem IPSec-VPN sieht das wie folgt aus (SSL-VPN weisen ähnliche Probleme auf):



Herkömmliche VPN generieren separate Frames mit Protokoll-Overhead für jede Anwendung

Dabei werden normalerweise zwei separate Frames generiert: einer mit 100 Byte Daten (zzgl. Protokoll-Overhead) und einer mit 150 Byte (zzgl. Protokoll-Overhead). Anschließend muss jeder der Frames von der Gegenstelle separat als empfangen bestätigt werden, wodurch insgesamt vier Frames erforderlich sind, um die 250 Byte Daten über eine drahtlose Verbindung zu übertragen.

Bei Verwendung von Mobility XE sieht dasselbe Beispiel folgendermaßen aus: Die Daten von Anwendung A (100 Byte) und Anwendung B (150 Byte) werden gemeinsam in einem 250 Byte großen Paket (zzgl. Protokoll-Overhead) übertragen. Anschließend wird nur eine Bestätigung generiert, weshalb nur zwei Frames erforderlich sind, um dieselben 250 Byte Daten zu übertragen. Mobility wird dabei noch effizienter, wenn noch mehr Anwendungen Daten übertragen.



Verringerte und synchronisierte Neuübertragungen

Ein Großteil der mangelhaften Leistung bei WWAN-Verbindungen ist übermäßig aggressiven Neuübertragungs-Richtlinien zuzuschreiben. Die meisten IP-basierten Implementierungen wurden auf die Verwendung in Umgebungen mit hoher Bandbreite und geringen Verlusten abgestimmt (z. B. verkabelte Infrastrukturen). Bei WWAN-Verbindungen kommt es jedoch zu schwankenden Latenzzeiten, was von herkömmlichen Implementierungen leicht als Paketverlust fehlverstanden werden kann. Das Transportprotokoll sorgt dann für die überflüssige Neuübertragung eines vorangegangenen Frames.

Diese erneute Übertragung beeinträchtigt die Leistung in zweierlei Hinsicht:

- Daten werden doppelt über eine Verbindung übertragen, die ohnehin eine geringe Bandbreite besitzt. Diese unnötige Neuübertragung verbraucht die kostbaren Ressourcen einer durchsatzschwachen Verbindung und verzögert die Übertragung neuer Daten und Bestätigungen für übertragene Daten.
- Wenn ein Frame erneut übertragen wird, wird dabei in der Regel davon ausgegangen, dass der Verlust durch einen Netzwerkengpass entstanden ist, weshalb ein Backoff-Algorithmus zum Einsatz kommt, der die Gesamtmenge der gleichzeitig übertragbaren Daten begrenzt.

Durch die Verlängerung der tatsächlichen Neuübertragungsdauer bei wirklich verlorenen Frames wird die Wiederherstellungsdauer deutlich verlängert, was die Gesamtleistung ohne triftigen Grund verringert. Dies kann zu einem Spiraleffekt führen, der die Datenübertragung immer weiter verzögert – bis hin zu einem regelrechten Stop-and-Wait-Datenaustausch.

Mobility XE nutzt neben den standardmäßigen Roundtrip-Berechnungen noch zahlreiche heuristische Methoden zur Ermittlung der Netzwerklatenz. Diese zusätzlichen Berechnungen ermöglichen es Mobility, die Übertragung schneller an die schwankenden Latenzzeiten und sonstigen Bedingungen von WWANs anzupassen. Mobility verringert die Menge an doppelt gesendeten Daten erheblich und ermöglicht dadurch die Übertragung von mehr Anwendungsdaten über die vorhandene Bandbreite.

Ein einfaches, aber deutliches Beispiel für diese heuristischen Methoden ist die Richtlinie für die synchronisierte Neuübertragung von Mobility XE. Wenn bei herkömmlichen Implementierungen ein Frame übertragen wird, wird ein Zeitlimit für die Empfangsbestätigung des Frames gesetzt. Geht diese Empfangsbestätigung nicht ein, wird von einigen Systemen einfach blind eine Kopie des Frames übertragen. Wenn Mobility hingegen entscheidet, dass eine Neuübertragung erforderlich ist, überprüft es zunächst, ob die zugrunde liegende Netzwerkschicht die vorherige Kopie des Frames

Technischer Überblick für Systemadministratoren

verarbeitet hat. Ist dies nicht der Fall, wird die Übermittlung einer neuen Kopie verzögert. Falls sich ein mobiles Gerät beispielsweise vorübergehend außer Reichweite befindet, ist es nicht erforderlich, eine weitere Kopie zu senden, wenn die vorherige das lokale System noch nicht einmal verlassen hat.

Ein weiteres Beispiel für die erweiterten Funktionen von Mobility XE ist seine Fähigkeit, Informationen über die Verbindungsqualität anwendungsübergreifend auszutauschen.

Aktuelle Transportimplementierungen funktionieren wie folgt:

- Da jede Anwendung eine Verbindung zu einer Gegenstelle aufbaut, ermittelt der Transportmechanismus die Eigenschaften der Verbindung.
- Sobald diese Daten vorliegen, steigt die Verbindungsleistung. Allerdings dauert es eine Weile, bis genügend Anwendungsdaten (in der Regel mindestens 64 KB) die Verbindung passiert haben.
- Bei Beendigung der Verbindung gehen die gesamten ermittelten Informationen verloren.

Mobility XE arbeitet hingegen folgendermaßen:

- Mobility XE speichert die ermittelten Informationen. Wenn eine Anwendung eine neue Verbindung herstellt, werden für diese Verbindung zunächst die zuletzt verwendeten Parametereinstellungen verwendet.
- Wenn Mobility XE von einem Netzwerk in ein anderes wechselt, werden die neuen Eigenschaften gleichzeitig auf alle aktiven Verbindungen angewendet. So müssen diese Werte nicht für jede Verbindung einzeln berechnet werden, was möglicherweise zusätzliche Neuübertragungen verursachen würde.

Fragmentierungsoptimierung

Die Fragmentierung von IP-Paketen wird von Netzwerkbenutzern als notwendiges Übel betrachtet, dem man entgegenwirken sollte. Die Fragmentierung verschwendet Ressourcen auf zahlreiche Weisen:

- Ein zwischengeschaltetes System (z. B. ein Router) muss ggf. zusätzlichen Verarbeitungsaufwand für fragmentierte Frames leisten und kann diese nicht einfach an ihr eigentliches Ziel weiterleiten.
- Auf dem empfangenden System kann es erhebliche Ressourcen in Anspruch nehmen, einen Frame wieder zusammzusetzen.
- Wenn auch nur ein Teil des fragmentierten Frames verloren geht, muss der gesamte Frame erneut übertragen werden.

Beim Wechsel von einem Netzwerk zum anderen (und einer damit verbundenen möglichen Änderung der Frame-Größe) kann Fragmentierung jedoch erforderlich sein. Mobility XE optimiert diese wie folgt:

- Es gibt eine bestimmte Maximalgröße für Nachrichten, die über eine Verbindung übertragen werden, und diese ist Mobility XE bekannt. Wenn die Anwendung nun eine Anforderung zur Übertragung von Daten sendet, die zu groß für eine einzelne Nachricht sind, werden die Daten vor der Übergabe an die darunter liegende Netzwerkschicht fragmentiert. Diese Vorgehensweise hat den Vorteil, dass die Daten das Netzwerk als „normale“ (unfragmentierte) Frames durchlaufen und keinen zusätzlichen Overhead bei zwischengeschalteten Systemen erzeugen.

- Der Nachrichtenfragmentierungs-Algorithmus von Mobility XE wurde dahingehend optimiert, dass möglichst wenig Ressourcen (sowohl hinsichtlich der Prozessorleistung als auch des Speicherbedarfs) zur Fragmentierung und Defragmentierung von Nachrichten erforderlich sind. Im Falle einer Neuübertragung wird auch die erforderliche Fragmentierung erneut berechnet. Falls sich die maximal mögliche Nachrichtengröße inzwischen erhöht hat, wird der Frame also ggf. bei der Neuübertragung unfragmentiert übertragen, was erneut Netzwerk-Overhead einspart.

Datenkomprimierung

Durch Datenkomprimierung kann der Durchsatz von Verbindungen mit geringer Bandbreite oder in stark ausgelasteten Netzwerkumgebungen verbessert werden, was dem Kunden – abhängig von den nutzungsabhängigen Netzwerkkosten – viel Zeit und Geld sparen kann. Mit Mobility XE kann der Systemadministrator die Komprimierungsfunktionalität individuell anpassen und festlegen, wann sie verwendet werden sollte bzw. ob sie generell (für alle Benutzer und Geräte), für eine bestimmte Art von mobilen Geräten, für ein bestimmtes Gerät oder für einen einzelnen Benutzer genutzt werden soll. Alternativ kann Mobility auch so konfiguriert werden, dass es die Komprimierung abhängig von der aktuellen Schnittstellengeschwindigkeit automatisch aktiviert oder deaktiviert. Benutzer können so zwischen durchsatzstarken 802.11b-LAN-Verbindungen und langsameren GPRS- oder 1xEV-DO-WAN-Verbindungen wechseln und erhalten automatisch die bestmögliche Leistung.

Mobility XE komprimiert Daten, die zwischen dem Mobility-Server und -Client ausgetauscht werden. Dabei kommen die in RFC 1951 (LZ77 Deflate/Inflate) beschriebenen Standardalgorithmen zum Einsatz. Übrigens werden nur die eigentlichen Anwendungsdaten in jedem Frame komprimiert. Die Transport-Header bleiben unangetastet. Dadurch kann Mobility Daten durch beliebige Einrichtungen zur Richtliniendurchsetzung senden, beispielsweise durch Firewalls oder NAT-Komponenten (Network Address Translation). Zudem funktioniert es in jedem beliebigen IP-basierten Netzwerk.

Im Gegensatz zu anderen Komprimierungstechnologien, die auf bestimmte Anwendungen spezialisiert sind, wird die Mobility XE-Implementierung auf alle Daten auf Anwendungsebene angewendet, die den Mobility-Tunnel passieren. Zur Nutzung dieser Funktionalität muss die Anwendung weder geändert noch speziell konfiguriert werden. Der Overhead für Wörterbuch- und sonstige organisatorische Zwecke beläuft sich bei Client und Server auf weniger als 16 KB pro Mobility-Verbindung. Es ist dabei jedoch schwer vorhersagbar, wie stark die Daten komprimiert werden, da dies von der Art der gesendeten Daten abhängig ist.

Siehe hierzu auch die Ausführungen in RFC 1951, in denen es sinngemäß heißt: „Ein einfaches Zahlenbeispiel zeigt, dass kein verlustloser Komprimierungsalgorithmus jede beliebige Art von Daten komprimieren kann. Englischer Text wird in der Regel um den Faktor 2,5 bis 3 komprimiert, Programmdateien lassen sich meist weniger stark komprimieren, Grafikdaten wie Rasterbilder wiederum bisweilen viel stärker.“

Mit anderen Worten, die Effektivität der Komprimierung ist Schwankungen unterworfen. Mobility XE hält sich dabei auch an die in RFC 1951 definierte Richtlinie, dass die Menge der übertragenen Daten nicht wachsen darf.

Da der Komprimierungsvorgang beträchtliche Rechenleistung beansprucht, muss ein Kompromiss gefunden werden, der einen größtmöglichen Nutzen für den Benutzer sicherstellt. Als Faustregel kann gelten, dass bei einer durchgängigen

Übertragungsgeschwindigkeit von über einem Megabit pro Sekunde keine erheblichen Einsparungen durch Komprimierung zu erwarten sind. Mobility XE berücksichtigt dies und nutzt weitere ausgefeilte Algorithmen zur Ermittlung von Netzwerklatenz und Komprimierungsraten. Auf der Grundlage der Netzwerklatenz und des Prozentsatzes an Einsparungen, der sich durch die Übertragung eines komprimierten Frames im Gegensatz zur Übertragung des Original-Frames erzielen lässt, legt Mobility ggf. fest, dass es sinnvoller ist, einen Frame unkomprimiert zu übertragen. Dies verringert die Prozessorleistung, die zur Dekomprimierung des Frames beim Empfang erforderlich ist, und bietet dem Benutzer somit den größten Nutzen. Wie in allen anderen Fällen auch, ist die Nutzung der Netzwerk- und Rechnerressourcen durch Mobility dabei so effizient wie möglich.

Web-Beschleunigung

Zur Beschleunigung des Surfens im Internet über langsame Netzwerke bietet Mobility XE die Option, Bilder zu komprimieren. Der Grad der Komprimierung ist konfigurierbar und die Komprimierung kann in Verbindung mit dem mobilen VPN von Mobility XE genutzt werden (im Gegensatz zu den Webbeschleunigungs-Lösungen der meisten Mobilfunkbetreiber, die sich nicht zusammen mit einem VPN nutzen lassen):

- JPEG-Bilder werden mithilfe der JPEG-Algorithmen komprimiert (die schnellste Einstellung erzielt Dateigrößen von etwa 28 Prozent der Originalgröße).
- Bei GIF-Bildern wird die Anzahl der Bit pro Pixel verringert, wodurch sich die Anzahl der Farben verringert. Außerdem wird das Bild auf eine einzige Ebene reduziert: Animierte GIFs werden zu einem einzigen Bild reduziert und Textanmerkungen werden entfernt.

Die Web-Beschleunigung ist an zwei unterschiedlichen Stellen verfügbar:

- Richtlinienverwaltungsmodul: Mithilfe von Richtlinien kann der Administrator die Web-Beschleunigung selektiv aktivieren und deaktivieren oder die HTTP-Ports basierend auf den aktuellen Netzwerkeigenschaften, einer spezifischen Anwendung oder beliebigen der sonstigen zur Verfügung stehenden Bedingungen ändern.
- Client-Einstellungen: Die Web-Beschleunigung ist bereits in der Lizenz für das Hauptprodukt enthalten. Der Grad der Komprimierung lässt sich einstellen. Ist die Komprimierung aktiv, werden beim gesamten HTTP-Verkehr, der über die angegebenen Ports läuft, die Bilder entsprechend den Einstellungen komprimiert.

Paketgrößen

Die TCP/IP-Paketgrößen sind für die drahtlose Übertragung nicht immer ideal. In einer Drahtlosumgebung steigt die Fehlerquote mit sinkender Übertragungsleistung und das heißt, dass es in Bereichen mit schlechtem Empfang viel häufiger zu Fehlern kommt. Wenn in diesen Situationen große Pakete übertragen werden, steigt die Wahrscheinlichkeit, dass ein ganzes Paket neu übertragen werden muss. Kleinere Pakete können hier die Gesamteffizienz steigern, weil sie die Anzahl der Übertragungswiederholungen senken. Viele Netzwerkadministratoren sind sich dessen nicht bewusst, dass es selbst in WLANs zu einer erheblichen Anzahl an verlorenen Paketen und Paketfehlern kommen kann.

Das UDP-Protokoll ist für Drahtlosnetze wesentlich besser geeignet. Es vermeidet den Overhead und die Ineffizienz von TCP, einem Protokoll, das nicht für Drahtlosnetze konzipiert wurde. Statt dessen liegt das Internet Mobility-Protokoll von Mobility über dem

UDP und implementiert seine eigenen Methoden zur dynamischen Einstellung der Paketgröße und der Timing-Parameter in Abhängigkeit von den Netzwerkbedingungen. IMP bewältigt im Zusammenspiel mit UDP die viel stärker schwankenden Übertragungsgeschwindigkeiten und Verbindungsbedingungen, die in Drahtlosnetzen auftreten. Dieser Ansatz ermöglicht IMP auch die Anwendung seiner eigenen Komprimierungs- und Verbindungsoptimierung, die den Durchsatz bei Netzwerken mit beschränkter Bandbreite verdoppeln kann.

Zuverlässigkeit

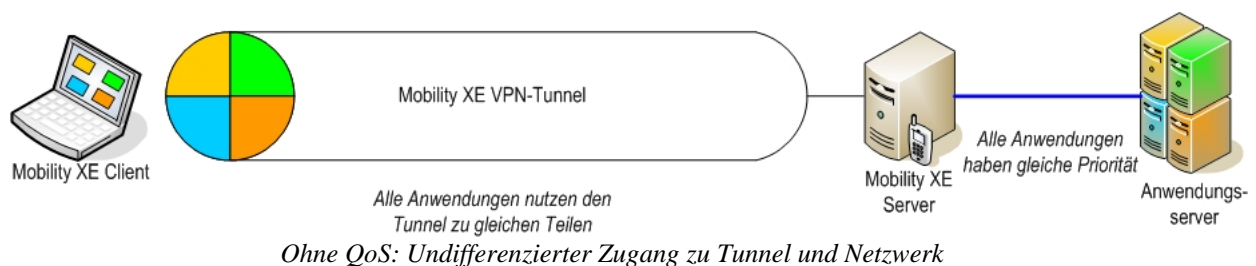
Da das UDP-Protokoll verbindungslos ist, übernimmt das Internet Mobility-Protokoll von Mobility diese Aufgabe zur Gewährleistung einer zuverlässigen Datenlieferung. Es verwendet einen eigenen Algorithmus, um Pakete selektiv zu quittieren, Zeitüberschreitungen zu handhaben, verlorene Pakete zu erkennen und diese neu zu übertragen. IMP ist wesentlich fortschrittlicher als TCP/IP, was auch erforderlich ist. Es muss nicht nur trotz der Ungewissheit in einer Drahtlosumgebung die Lieferung von Paketen überprüfen, sondern dies mit einem minimalen Overhead und möglichst wenigen erneut übertragenen Frames bewerkstelligen, ohne zu viel Bandbreite in Anspruch zu nehmen.

Traffic Shaping

Quality of Service und DSCP

Mobility XE implementiert mithilfe des Richtlinienverwaltungsmoduls (siehe unten) ausgefeiltes Quality of Service (QoS), um die Parameter festzulegen, nach denen der Netzwerkverkehr priorisiert und „geformt“ werden soll. QoS ist von größter Bedeutung, um die Produktivität aufrechtzuerhalten, wenn Mitarbeiter von Hochgeschwindigkeits-Netzwerken mit hoher Bandbreite in Netzwerke mit geringerer Kapazität und höheren Latenzzeiten wechseln. Möglicherweise reicht bei Ethernet-LAN-Verbindungen zum Beispiel die Leistung für die Ausführung geschäftskritischer Unternehmensanwendungen oder das Führen eines VoIP-Telefongesprächs (Voice-over-IP) und die gleichzeitige Verwendung von E-Mail-, Browser- und anderen Anwendungen vollkommen aus. Bei Verwendung eines WWAN aber sollten Administratoren Prioritäten zur Nutzung der geringeren Bandbreite setzen und gewährleisten, dass Webbrowser oder E-Mail-Clients keine Bandbreite in Anspruch nehmen, die für die Unternehmens- oder VoIP-Anwendungen benötigt wird.

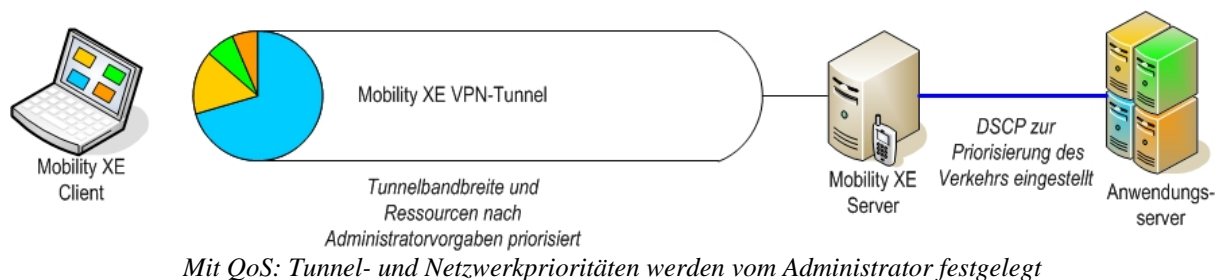
QoS spielt eine zentrale Rolle, da Sprach- und Videodaten einen größeren Anteil an den Netzwerkressourcen beanspruchen. Diese Anwendungen benötigen viel Bandbreite und sind auf eine schnelle und zuverlässige Paketübertragung angewiesen. Mithilfe von QoS-Richtlinien können Administratoren diesen Anwendungen die erforderliche Priorität geben, die sie für einen einwandfreien Betrieb benötigen.



Mobility XE nimmt eine grobe Klassifizierung der Verkehrspriorität in fünf Kategorien vor: „High Priority“ (Hohe Priorität), „Voice“ (Sprache), „Video“, „Best Effort“

(Durchschnittliche Priorität) und „Background“ (Hintergrund). Jede Klassifizierung besitzt eine vordefinierte Konfiguration für die verschiedenen QoS-relevanten Einstellungen, die eine sehr präzise Steuerung von Traffic Shaping, Verhalten des Packet Queuing, Timing, DSCP-Tagging (Differential Service Code Point) und anderer erforderlicher Mechanismen ermöglichen. Beispielsweise kann dem VoIP-Verkehr, falls er wichtig ist, die Priorität „Voice“ (Sprache) zugewiesen werden, um ein optimales Traffic Shaping zu erzielen, oder Sie können ihm die Priorität „Best Effort“ (Durchschnittliche Priorität) oder „Background“ (Hintergrund) zuweisen, falls er keinen wichtigen Stellenwert bei der Verwendung des Netzwerks einnimmt.

Mobility XE ermöglicht unterschiedliche Einstellungen auf der Grundlage spezifischer Anwendungen oder IP-Adressen. Diese umfassenden Steuerungsmöglichkeiten für die Netzwerknutzung sind das Markenzeichen des Mobility XE Mobile VPN. Bei herkömmlichen VPN haben die Administratoren häufig nur die Möglichkeit, weniger wichtige Anwendungen zu deaktivieren. Bei Mobility XE können die Anwendungen hingegen mit geringer Priorität weiterlaufen. Sobald die Anwendungen mit höchster Priorität die Datenübertragung beendet haben, wird dann der vollständige Zugang zum Netzwerktunnel automatisch wieder für die restlichen Anwendungen freigegeben.



Wenn QoS aktiviert ist, wirken sich seine Regeln auf den gesamten Verkehr aus, der den Tunnel von Mobility XE passiert. Auf der privaten/internen Seite des Mobility-Servers unterstützt Mobility XE den Internet-Standard des DSCP-Taggings, das das Routing von Daten durch Infrastrukturkomponenten wie Router oder Firewalls anhand von TOS-Bits (Type of Service) im TCP/IP-Paket-Header priorisiert.

PLR (Packet-Loss Recovery)

PLR (Packet-Loss Recovery, Wiederherstellung verlorener Pakete) ist Teil des QoS-Mechanismus von Mobility XE und erweist sich insbesondere bei Mediendatenströmen wie Sprache oder Video als sehr nützlich. Diese Datenströme erfordern eine fortlaufende, zeitkritische Paketübertragung in der richtigen Reihenfolge. Da die erneute Übertragung eines Pakets zu lange dauern würde, führen Paketverluste insbesondere bei Drahtlosnetzwerken mit geringer Bandbreite, hohen Latenzzeiten und viel Jitter zu kurzen Bild- oder Gesprächsunterbrechungen. Die PLR-Technik, die von den QoS-Richtlinien von Mobility XE QoS angewendet wird, nutzt ein ausgeklügeltes mathematische Modell, das jedes Paket um einen geringen Overhead erweitert. Gehen Pakete verloren, werden sie von PLR anhand der Daten in den empfangenen Paketen rekonstruiert. Administratoren können den Wirkungsgrad von PLR dabei so anpassen, dass ein ausgewogenes Verhältnis aus Rekonstruktionsanforderungen und Netzwerkbedingungen bzw. dem generierten zusätzlichen Datenverkehr pro Paket erzielt wird. Bei einer niedrigen PLR-Einstellung werden weniger Daten hinzugefügt, was in der Regel für Situationen mit geringen Paketverlusten ausreichend ist. Eine hohe PLR-Einstellung ermöglicht eine effektivere Rekonstruktion, erhöht aber die Menge des Overheads pro Paket. PLR wird über die Einstellungen zur QoS-Richtlinienverwaltung aktiviert und standardmäßig auf Verkehr angewendet, der als Sprach- oder Videodaten klassifiziert ist. Als Standardeinstellung wird für PLR die mittlere Einstellung verwendet.

Verwaltung

Richtlinienverwaltung

Der Mobility-Server verwaltet Benutzerrichtlinien und überträgt diese im Push-Verfahren an die Mobility-Clients, wo diese Richtlinien durchgesetzt werden. Richtliniendokumente werden im Mobility-Datenspeicher aufbewahrt. Alle Mobility-Server in einer Servergruppe verwenden gemeinsame Richtlinien.

Die Mobility-Richtlinien werden im Push-Verfahren an die mobilen Geräte übertragen, wenn diese eine Verbindung herstellen. Richtlinien können für spezifische Geräte oder Benutzer definiert werden. Richtlinienaktualisierungen und -änderungen werden in Echtzeit vorgenommen, nachdem der Administrator sie zur Verteilung veröffentlicht.

Für die Speicherung, den Aufruf und die Validierung von Regeln zwischen Client und Server verwendet Mobility eine XML-basierte Regelsprache. Ein Richtliniendokument enthält die XML-Definition der Richtlinie als geordnete Liste von Regeln, die aus dem Regeldokument stammen (eine Regel oder ein Satz Regeln, der das Verhalten des Client-Netzwerks steuert). Der Mobility-Server analysiert den ausführlichen serverseitigen XML-Code und macht daraus nutzbare Codeobjekte. Die Regeln werden anhand einer XSD (XML-Schemadefinition) validiert, wenn das erzeugte Dokument gespeichert oder geöffnet wird. Wenn Regeln erstellt und gespeichert werden, wird eine XSL-Transformation des ausführlichen serverseitigen XML-Codes in das Client-Format vorgenommen, wodurch ein ressourcenschonendes Richtliniendokument entsteht, das nur die Informationen enthält, die der jeweilige Client benötigt.

Die Richtlinien ermöglichen eine extrem flexible und präzise Steuerung des Zugriffs von Benutzer und Gerät auf die Netzwerkressourcen. Dabei werden die Regeln auf Geräteebene durchgesetzt, die Regelsätze in für Menschen lesbarer Form befinden sich jedoch auf dem Mobility-Server.

Durchsetzen von Richtlinien

Folgende grundlegende Maßnahmen der Richtlinienverwaltung haben Auswirkungen auf Verbindungen: „Allow“ (Zulassen), „Block“ (Blockieren), „Disconnect“ (Trennen) und „Passthrough“ (Durchleiten). Mobility XE setzt diese Maßnahmen auf der Client-Seite durch. Wenn eine Anwendung versucht, Daten über das Netzwerk zu senden, prüft der Mobility-Client die Richtlinienliste für die Anwendung, den Port, die Zieladresse und andere Parameter, um zu ermitteln, wie er vorgehen sollte. Bei den nachfolgenden Beschreibungen wird davon ausgegangen, dass die beschriebenen Maßnahmen jeweils die Basismaßnahmen der Richtlinie sind. Das Verhalten kann sich ändern, wenn die Maßnahme aufgerufen wird, nachdem eine Sitzung aktiviert wurde.

Maßnahme	Beschreibung
Allow (Zulassen)	Wenn die Richtlinienmaßnahme „Allow“ (Zulassen) ist, gibt der Mobility-Client die Anforderung an den Mobility-Server und dann an das Ziel weiter.
Block (Blockieren)	Wenn die Maßnahme „Block“ (Blockieren) ist, legt der Mobility-Client den E/A-Status der Verbindungsanforderung auf der TDI-Schicht als wartend fest. Die Winsock-Schnittstelle sendet eine entsprechende Antwort an die Anwendung, die der verwendeten E/A-Methode entspricht. Für die Anwendung sieht es daher so aus, als wäre die Sitzung noch aktiv.
Disconnect (Trennen)	Falls es sich bei der Maßnahme um „Disconnect“ (Trennen) handelt, sendet der Mobility-Client einen Hinweis an die Winsock-Schnittstelle, dass der Server am anderen Ende den Befehl zum Trennen gegeben hat. Dadurch scheint es, dass der Server am anderen Ende die Verbindung beendet hat und die Sitzung wird beendet.
Passthrough (Durchleiten)	Wenn die Maßnahme „Passthrough“ (Durchleiten) ist, leitet der Mobility-Client den Verkehr direkt zur TCP/IP-Transportschicht durch, damit er als normaler TCP/IP-Verkehr außerhalb des verschlüsselten Tunnels zwischen dem Mobility-Client und -Server weitergeleitet wird.
Set QoS Parameters (QoS-Parameter festlegen)	Falls es sich bei der Maßnahme um „Set Quality of Service parameters“ (QoS-Parameter festlegen) handelt, priorisiert der Mobility-Client den Verkehr, während dieser den VPN-Tunnel passiert, unter Anwendung der vorgegebenen Einstellungen.

Die Richtlinienverwaltung ermöglicht die präzise Verwaltung der Bandbreite von Drahtlosnetzwerken, der Sicherheit und der Produktivität von mobilen Benutzern – ohne Umwege oder hohe Kosten und selbst bei Netzwerken, die der Administrator nicht beeinflussen kann.

Netzwerkzugangskontrolle (NAC)

Das Mobile NAC-Modul überprüft, ob die Sicherheitsmaßnahmen aktiviert und auf dem neuesten Stand sind und ob das Gerät entsprechend den definierten Richtlinien konfiguriert ist. Abhängig davon, wie viele der NAC-Richtlinien vom Gerät nicht erfüllt werden, können unterschiedlichste Schritte eingeleitet werden: Möglicherweise werden nur einfache Warnungen ausgegeben oder es wird die Behebung der Schwachstellen durchgesetzt, es kann aber auch die Verbindung zum Gerät getrennt oder das Gerät unter Quarantäne gestellt werden.

Die NetMotion Mobile NAC unterscheidet sich von der herkömmlichen NAC durch seine Fähigkeit, die Produktivität der Mitarbeiter aufrechtzuerhalten, indem die Reaktion auf einen Client, der die Richtlinien nicht erfüllt, angepasst wird. Ein Mitarbeiter im Außendienst sollte nicht immer dazu gezwungen werden, seinen Arbeitstag zu unterbrechen, weil ein mittelschweres Sicherheitsproblem festgestellt wurde. Betriebssystemaktualisierungen und das Herunterladen von Virenschutzsignaturen, die

über ein Mobilfunknetz viele Minuten dauern würden, können auf das Ende des Arbeitstags verschoben und/oder ausgesetzt werden, bis der Mitarbeiter sich in einem Netz mit größerer Bandbreite befindet.

Administratoren können mithilfe des NAC-Moduls Richtlinien erstellen, die den Sicherheitsstand eines Client-Geräts überprüfen.

Kategorie	Überprüfte Parameter
Virenschutz und Spyware-Schutz	Vorhandensein des angegebenen Produkts, Aktivierung des Echtzeitschutzes, Stand der Signaturen, Datum und Ergebnis der letzten Prüfung
Datei	Vorhandensein der angegebenen Dateien auf dem Client
Firewall	Vorhandensein und Ausführung des angegebenen Produkts
Prozess	Ausführung der angegebenen Anwendung bzw. des angegebenen Diensts
Registrierungsschlüssel	Vorhandensein von Schlüsseln im Abschnitt HKEY_LOCAL_MACHINE\ der Registrierung, Prüfung auf erforderliche Werte
Windows-Aktualisierung	Aktivierung der automatischen Aktualisierung und/oder Vorhandensein bestimmter Patches
Mobility-Version	Version des Mobility-Clients
Betriebssystem	Version des Betriebssystems, Service Pack, Prozessor und weitere Plattformdaten

Das NAC-Modul funktioniert sehr ähnlich wie das Richtlinienmodul. Der Mobility-Server speichert die NAC-Regeln und sendet sie im Push-Verfahren an jedes Gerät, das eine Verbindung herstellt. Der Mobility-Client auf dem jeweiligen Gerät überprüft die Erfüllung der NAC-Richtlinien beim Verbindungsaufbau und in regelmäßigen Abständen (standardmäßig alle fünf Minuten).

Durchsetzen der NAC-Richtlinien

Wenn ein Client-Gerät eine NAC-Richtlinienprüfung nicht besteht, kann ihm eine von fünf Statuskategorien zugewiesen werden.

Status	Beschreibung/Maßnahme
Warn (Warnen)	Der Client erfüllt einen oder mehrere Aspekte einer Regel nicht. Das Mobility-Client-Gerät darf eine Verbindung aufbauen, der Mobility-Client zeigt jedoch eine Warnung an.
Remediate (Beheben)	Der Client erfüllt einen oder mehrere Aspekte einer Regel nicht, bei der die Behebung von Schwachstellen erforderlich ist. Die Maßnahme, die erforderlich ist, damit das Gerät wieder den Richtlinien entspricht, wird anhand von Richtlinienverwaltungsregeln ermittelt.
Disconnect (Trennen)	Der Client erfüllt einen oder mehrere Aspekte einer Regel nicht, bei der die Verbindung zum Client getrennt werden muss.
Quarantine (Unter Quarantäne stellen)	Der Client erfüllt einen oder mehrere Aspekte einer Regel nicht, bei der das Gerät unter Quarantäne gestellt werden muss. Der Systemadministrator muss die Quarantäne aufheben, damit das Gerät sich wieder verbinden kann.

Wenn der Status „Remediate“ (Beheben) lautet und sowohl das NAC- als auch das Richtlinienmodul eine aktive Lizenz auf dem Mobility-Server besitzen, stehen dem Administrator mehrere flexible Optionen zur Verfügung. Beispielsweise kann er eine bestimmte Maßnahme auf Grundlage der aktuellen Verbindungsgeschwindigkeit, der Tageszeit usw. einleiten. Ein typisches Beispiel könnte wie folgt aussehen: Wenn die Virenschutzsignaturen über sieben Tage alt sind, wird eine Aktualisierungs-Erinnerungsmeldung gesendet. Sind sie über 14 Tage alt und es besteht eine WWAN-Verbindung, wird ein Hinweis gesendet, dass die Signaturen baldmöglichst aktualisiert werden müssen. Falls sie über 14 Tage alt sind und eine Wi-Fi- oder LAN-Verbindung besteht, werden unmittelbar neue Signaturen heruntergeladen. Sind die Signaturen über 21 Tage alt, wird das Gerät automatisch unter Quarantäne gestellt. Diese Funktionalität lässt sich auch dazu einsetzen, um automatisch Aktualisierungen und Betriebssystem-Patches zum Schutz von Gerät und Netzwerk zu einem Zeitpunkt herunterzuladen und zu aktualisieren, zu dem sie nicht die Produktivität der Mitarbeiter stören.

Client-Aktivität/Mobility-Konsole

Der Mobility-Server erfasst zahlreiche verschiedene Details zur Sitzung des aktiven Geräts:

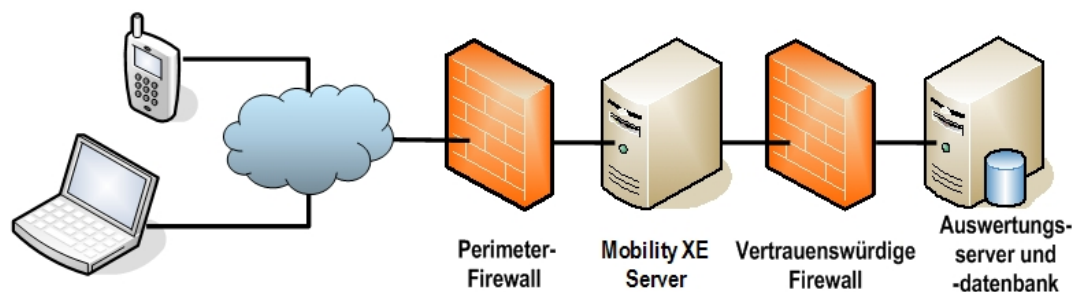
- Gerätename
- Benutzername
- Client-Status
- Gerätebeschreibung
- Geräteklasse und -ID
- Servername
- Virtuelle Adresse
- POP-Adresse
- Gesendete Bytes
- Empfangene Bytes
- Registrierung des Clients (Datum/Uhrzeit)
- Verbindungsaufbau (Datum/Uhrzeit)
- Gesamt-Verbindungsdauer
- Client-Version
- Betriebssystem des Clients
- Client (angedockt oder nicht)
- Stromversorgung (Akku/Netz)
- Akku (verbleibende Leistung in Prozent)
- SSID des Drahtloszugangspunkts
- BSSID des Drahtloszugangspunkts
- Anwendungen, die das Netzwerk nutzen (gesendete/empfangene Bytes)

Bei der erstmaligen Verbindung überträgt der Mobility-Client die Sitzungsinformationen an den Mobility-Server, der die Sitzungsdatenseite der Mobility-Konsole (für alle verbundenen Geräte) mit diesen Informationen ausfüllt. Wenn der Verbindungszustand auf der Datenseite aufgezeichnet ist, werden die Informationen bei Änderungen bzw. in regelmäßigen Abständen aktualisiert. Die POP-Adresdaten ändern sich beispielsweise nur, wenn das Gerät das Netzwerk wechselt. Wenn das mobile Gerät eine neue POP-Adresse bezieht, informiert der Mobility-Client den Mobility-Server über die neuen Sitzungsdaten. Wenn sich keine anderen Informationen geändert haben, werden diese auch nicht übertragen. Informationen, die häufiger aktualisiert werden müssen, wie z. B. der Batterieladezustand des Geräts, werden nach konfigurierbaren Zeitvorgaben aktualisiert.

Da der Mobility-Server für jeden Mobility-Client als Proxy für den Anwendungsverkehr fungiert, kann die Anzahl der pro Anwendung (Prozess) gesendeten Bytes vom Mobility-Server abgefragt werden, ohne dass der Client oder das Netzwerk mit der Übertragung dieser Informationen belastet werden muss.

Analytics Module

Das Analytics Module erweitert Mobility-Installationen um Auswertungs- und Benachrichtigungsfunktionen. Hierfür sind zwei zusätzliche Komponenten erforderlich: ein Auswertungsserver und eine Auswertungsdatenbank. Der Auswertungsserver sammelt die Daten aller Mobility-Server in einem Pool und leitet die Daten zur Archivierung und für Abfragen an die Datenbank weiter. Der Auswertungsserver überwacht zudem verschiedene Systembedingungen und sendet Benachrichtigungen, wenn er eine dieser Bedingungen erkennt. In der Datenbank werden die Daten in standardisierter Form gesammelt, wodurch sie umgehend zur Auswertung bereitstehen.



Das Analytics Module erfasst statistische Verhaltens- und Nutzungsdaten zu Benutzer, Gerät und Netzwerk.

Da der Mobility XE Server als Proxy für Anwendungen fungiert und jeder Mobility-Client seine Drahtlosverbindungen verwaltet, kann der Auswertungsserver die Ressourcennutzung durch mobile Geräte in höchst detaillierter Form erfassen. Dies geht weit über die Überwachung von Verbindungen und An-/Abmeldeereignissen hinaus. Es umfasst beispielsweise Informationen dazu, welche Anwendungen verwendet wurden, wie viele Bytes pro Anwendung und insgesamt übertragen wurden und welchen Namen die Drahtlosschnittstelle hat (woraus ersichtlich ist, welches Netzwerk verwendet wurde). Die erfassten Daten bieten einen detaillierten Einblick in die Nutzung der einzelnen Geräte, Anwendungen und Netzwerke, aber auch in die Bandbreitennutzung oder die Verbindungsmuster und sogar bis hin zur Akkulaufzeit. Da viele dieser Informationen bereits aufgrund der Funktion des Mobility-Servers als Anwendungs-Proxy zur Verfügung steht, entsteht durch das Analytics Module nur eine sehr geringe Menge an Overhead in Drahtlosnetzwerken. Es erfasst und analysiert einfach die Daten, um sie zugänglich und praktisch nutzbar zu machen.

Technischer Überblick für Systemadministratoren

23

Wenn die Daten eintreffen, werden sie vom Auswertungsserver anhand vom Administrator definierter Bedingungen analysiert und wenn eine dieser Bedingungen zutrifft, wird eine Benachrichtigung ausgegeben. Diese Bedingungen dienen dazu, Unregelmäßigkeiten bei Verbindungen, Geräten, Drahtlosnetzwerken und der Implementierung von Mobility festzustellen. Für einige der Benachrichtigungen können vom Administrator Schwellenwerte festgelegt werden. Falls eine Bedingung, die eine Benachrichtigung ausgelöst hat, nicht mehr vorhanden ist, sendet der Auswertungsserver eine weitere Nachricht, um zu melden, dass die Situation kein unmittelbares Problem mehr darstellt. Außerdem wird in der Mobility-Konsole ein Bericht generiert, der alle Benachrichtigungen enthält, die im Laufe der Zeit ausgelöst wurden. Zusätzlich können Administratoren konfigurieren, ob eine automatische Benachrichtigung per E-Mail oder über einen SNMP-Manager oder Syslog-Dämon im Netzwerk erfolgen soll.

Bei der Auswertungsdatenbank handelt es sich um Microsoft SQL Server 2005 Express, eine Datenbank der Enterprise-Klasse, die bei weniger umfangreichen Implementierungen bis zu fünf Jahre an Berichtsdaten speichern kann. Kunden können auch ihre eigene lizenzierte Enterprise-Version von Microsoft SQL Server 2005 für die Auswertungsdatenbank verwenden. Das Analytics Module umfasst mehrere vordefinierte Berichte, auf die über die Mobility-Konsole zugegriffen werden kann. Die zugehörige Benutzeroberfläche zum selektiven Filtern der Daten ist sehr einfach zu bedienen. Auf diese Weise kann der Administrator Benutzer, Netzwerke, Anwendungen, Zeitabschnitte usw. gruppiert und einzeln betrachten.

Das komponentenbasierte Konzept hat den Vorteil, dass es die Auswertungsinfrastruktur vor Datenverlust schützt, wenn eine einzelne Komponente ausfällt. Falls beispielsweise der Server, auf dem die Auswertungsdatenbank gehostet wird, unerwartet vom Netzwerk getrennt wird, gibt er nicht nur eine Benachrichtigung aus, sondern empfängt auch weiterhin Daten vom Mobility-Server, die er in der Warteschlange speichert und weiterleitet, sobald die Verbindung wiederhergestellt ist.

Im Whitepaper zum *NetMotion Mobility XE Analytics Module* wird die Funktionalität des Analytics Module beschrieben. Dort finden Sie außerdem Beispiele und eine Liste der Berichte und Benachrichtigungen.

Zusätzliche Informationen

Zusätzliche Informationen finden Sie auf der Website von NetMotion Wireless, <http://www.netmotionwireless.com>, und im Systemadministrator-Handbuch.

© 2009 NetMotion Wireless Inc. Alle Rechte vorbehalten. NetMotion und NetMotion Mobility sind eingetragene Marken und Mobility XE, Roamable IPsec, InterNetwork Roaming, Best-Bandwidth Routing und Analytics Module sind Marken von NetMotion Wireless Inc. Microsoft, Microsoft Windows, Active Directory, ActiveSync, Internet Explorer, Windows Mobile, Windows Server, Windows XP, SQL Server, Windows XP Tablet PC Edition und Windows Vista sind eingetragene Marken der Microsoft Corporation. Alle übrigen Marken, Handels- oder Unternehmensnamen in diesem Dokument werden nur zu Identifizierungszwecken verwendet und sind Eigentum der jeweiligen Rechteinhaber. Die NetMotion-Technologie ist durch eines oder mehrere der folgenden US-Patente geschützt: 6,198,920, 6,418,324, 6,546,425, 6,826,405, 6,981,047, 7,136,645, 7,293,107 und das kanadische Patent 2,303,987. Weitere Patentanmeldungen in den USA und in anderen Ländern sind anhängig.