Manual abstract:

192 Testing the LA N path from your P C to a remote device . @@ 52 Figure 30: Protocol binding setup to associate a service and/or LAN source to a WAN and/or destination network . 53 Figure 31: Routing Mode is used to configure traffic routing between WAN and LAN, as well as Dynamic routing (RIP) . 69 Figure 42: List of A vailable Profiles shows the options available to secure the wireless link . 76 Figure 46: List of configured access points (Virtual APs) shows one enabled access point on the radio, broadcasting its SSID . 82 Figure 51: WPS configuration for an AP with WPA/WPA2 profile . 87 Figure 54: Example where an outbound SNAT rule is used to map an external IP address (209. 225) to a private DMZ IP address (10. 90 Figure 55: The firewall rule configuration page allows you to define the To/From zone, service, action, schedules, and specify source/destination IP addresses as needed. .
91 Figure 56: The IPv6 firewall rule configuration page allows you to define the To/From zone, service, action, schedules, and specify source/ destination IP addresses as needed. 98 Figure 61: A vailable ALG support on the router. 102 Figure 64: Content Filtering used to block access to proxy servers and prevent ActiveX controls from being downloaded. 106 Figure 68: The following example binds a LAN hostâ□□s MAC Address to an IP address served by DSR. If there is an IP/MAC Binding violation, the violating packet will be dropped and logs will be capt ured.
107 Figure 69: Intrusion Prevention features on the router . 108 Figure 70: Protecting the router and LAN from internet attacks . 109 Figure 71: Example of Gateway-to-Gateway IPsec VPN tunnel using two DSR routers connected to the Internet. 111 Figure 72: Example of three IPsec client connections to the internal network through the DSR IPsec gateway . 145 8 Unified Services Router User Manual Figure 98: Configured client routes only apply in split tunnel mode.
146 Figure 99: List of configured SSL VPN portals. The configured portal can then be associated with an aut hentication domain . 164 Figure 114: Log configuration options for traffic through router . 166 Figure 115: IP v6 Log configuration options for traffic through router . 170 Figure 119: Restoring configuration from a saved file will result in the current configuration being overwritten and a reboot . Th e s eco nd W AN p o rt can b e co n figu red as a DM Z p o rt allo win g y o u t o is o late s erv ers fro m y o u r LA N. Ty p ical d ep lo ymen t an d u se cas e s cen ario s are d es crib ed in each s ect io n . Fo r mo re d et ailed s et u p in s t ru ct io n s an d exp lan at io n s o f each co n fig u rat ion p aramet er, refer t o t h e o n lin e h elp t h at can b e acces s ed fro m each p ag e in t h e ro u t er GUI. Th e LA N co n n ectio n may b e t h ro u gh t h e wired Et h ern et p o rt s av ailab le o n t h e ro u t er, o r o n ce t h e in it ial s et up is co mp let e, t h e DSR may als o b e ma n ag ed t h ro u g h it s wireles s in t erface as it is b rid g ed wit h t h e LA N. W it h DHCP, PCs an d o t h er LA N d ev ices can b e assig ned IP ad d resses as well as ad d resses fo r DNS s erv ers , W in d o ws In t ern et Name Serv ice (W INS) s erv ers , an d t h e d efau lt g at eway .

Each p o o l ad dress is t ested b efore it is as sig ned t o av o id d u p licat e ad d res s es o n t h e LA N. Fo r mo s t ap p licat ion s t he d efault DHCP an d TCP/ IP s et t in g s are s at is fact o ry . if y o u wan t an o t h er PC o n y o u r n et wo rk t o b e t h e DHCP s erv er o r if y o u are man u ally co n fig u rin g t h e n et wo rk s et t in g s o f all o f y o u r PCs , s et t h e DHCP mo d e t o â□□n o n eâ□□. DHCP relay can b e u s ed t o fo rward DHCP leas e in fo rmat io n fro m an o t h er LA N d ev ice t h at is t h e n et wo rkâ□□s DHCP s erv er; t h is is p art icu larly u s efu l fo r wireles s clien t s . In s t ead o f u s in g a DNS s erv er, y o u can u s e a W in d o ws In t ern et Namin g Serv ice (W INS) s erv er. Yo u can als o en able DNS p ro xy fo r t h e LA N. In the LAN Setup page, enter the following information for your router: ï□· In the DHCP section, select the DHCP mode: ï□· Figure 1 : Se tup page for LAN TCP/IP s e ttings 15 Unified Services Router User Manual 2. 1. 1 LAN DHCP Reserv ed IPs Setup > Network Settings > LAN DHCP Reserved IPs Th is ro u t er DHCP s erv er can as sig n TCP/ IP co n fig urat io n s t o co mp u t ers in t h e LA N exp licit ly b y ad d in g clien t 's n etwo rk in t erface h ardware ad dress an d t he IP ad d ress t o b e as s ig ned t o t h at clien t in DHCP s erv er's d atabase. W h enever DHCP s erv er receiv es a req u est fro m c lien t , h ard ware ad dress o f t h at clien t is co mp ared wit h t h e h ard ware ad d res s lis t p res en t in t h e d at ab as e, if an IP ad d res s is alread y as s ig n ed t o t h at co mp u t er o r d ev ice in t h e d at ab as e , t h e cu s t o mized IP ad d res s is co n fig u red o t h erwis e an IP ad d ress is ass ig n ed t o t h e clien t au t o mat ically fro m t h e DHCP p o o l.
As s oci ate wi th IP/ MAC B i ndi ng : W h en t h e u s er en ab les t h is o p t io n t h e Co mp u t er Name, IP an d M A C ad d res s es are as s o ciat ed wit h t h e IP/ M A C b in d in g . Th e act io n s t h at can b e t aken o n lis t o f res erv ed IP ad d res s es are: S el ect: Select s all t h e res erv ed IP ad d res s es in t h e lis t . Th e fo llo win g s et t in g s are u s ed t o co n fig u re t h e DHCPv 6 s erv er: ï□· In t h is case t h e ro u ter ad vertis emen t d aemo n (RA DVD) mu s t b e co n fig u red o n t h is d ev ice an d ICM Pv 6 ro u t er d is co v ery mes s ag es are u s ed b y t h e h o s t fo r au t o -co n fig u rat io n . Prefix Delegation Th e fo llo win g s et t in g s are u s ed t o co n fig u re t h e Prefix Deleg at io n : ï□· 4 Configuring IPv 6 Router Adv ertisements Ro u t er A d v ertis emen ts are an alo go us t o IPv 4 DHCP as s ig nmen ts fo r LA N clien t s , in t h at t h e ro u t er will as s ig n an IP ad d res s an d s u p p o rt in g n et wo rk in fo rmat io n t o d ev ices t hat are co n fig ured t o accept s uch d etails. Th e fo llo win g s et t in g s are u s ed t o co n fig u re RA DVD: ï□· Th e act u al d u rat io n b et ween ad v ert is emen t s is a ran d o m v alu e b et ween o n e t h ird o f t h is field an d t h is field .
Figure 5 : Configu ri ng the Route r Adve rtis e me nt Dae mon Advertisement Prefixes Advanced > IPv6 > IPv6 LAN > Advertisement Prefixes Th e ro u t er ad v ert isemen ts co nfig ured wit h ad v ert is emen t p refixes allo w t h is ro u t er t o in fo rm h o s t s h o w t o p erfo rm s t at eles s ad d res s au t o co n fig u rat io n . ro u t er ad v ert is emen ts co n t ain a lis t o f s u b n et p refixes t h at allo w t h e ro u t er t o d et ermin e n eig h b o u rs an d wh et h er t h e h o s t is o n t h e s ame lin k as t h e ro u t er .

Th e fo llo win g p refix o p t io n s are av ailab le fo r t h e ro u t er ad v ert is emen t s : ï□· Figure 6 : IPv6 Adve rtis e me nt Pre fix s e ttings 2. LA N p o rt s can b e as s ig n ed u n iq u e VLA N IDs s o t h at t raffic t o an d fro m t h at p h y s ical p o rt can b e is o lat ed fro m t h e g en eral LA N. Figure 7 : Adding VLAN me mbe rs hips to the LAN 2.

By s elect in g o n e mo re VLA N memb ers h ip o p t io n s fo r a Gen eral o r Tru n k p o rt , t raffic can b e ro u t ed b et ween t h e s elect ed VLA N memb ers h ip IDs 25 Unified Services Router User Manual Figure 9 : Configu ri ng VLAN me mbe rs hip for a port 2. Each co n fig u red VLA N ID can map d irect ly t o a s u b n et wit h in t h e LA N. Each LA N p o rt can b e as s ig n ed a u n iq u e IP ad d ress an d a VLA N s p ecific DHCP s erv er can b e co nfig ured t o ass ig n IP ad d res s leas es t o d ev ices o n t h is VLA N. Th e DM Z ad d s an ad d it io n al lay er o f s ecu rit y t o t h e LA N, as s p ecific s erv ices/p ort s t h at are exp o s ed t o t h e in t ern et o n t h e DM Z d o n o t h av e t o b e exp o s ed o n t he LA N. Th ere are n o rest rictio ns on t h e IP ad d res s o r s u bnet as sign ed t o t h e DM Z p o rt , o t h er t h an t h e fact t h at it can n o t b e id en t ical t o t h e IP ad d res s g iv en t o t h e LA N in t erface o f t h is g at eway . If a n et wo rk d ev ice is d etect ed b y UPn P, t h e ro u t er can o p en in t ern al o r ext ern al p o rt s fo r t h e t raffic p ro t o co l req u ired b y t h at n et wo rk d ev ice. Figure 13 : UPnP Configuratio n UPn P Po rt map Tab le Th e UPn P Po rt map Tab le h as t h e d et ails o f UPn P d ev ices t hat res po nd t o t h e ro u terâ□□s ad v ert is emen t s . Th e fo llo win g in fo rmat io n is d is p lay ed fo r each d et ect ed d ev ice: ï□· A ct iv e: A y es /n o in d icatin g wh et her t he p o rt o f t h e UPn P d ev ice t hat es t ab lis h ed a co n n ect io n is cu rren t ly act iv e ï□· Po rt (Ext ern al Po rt): Th e ext ern al p o rt s o p en ed b y UPn P (if an y) IP A d d res s : Th e IP ad d res s o f t h e UPn P d ev ice d et ect ed b y t h is ro u t er Click Refres h t o refres h t h e p o rt map t ab le an d s earch fo r an y n ew UPn P d ev ices . Connecting to the Internet: WAN Setup Th is ro u t er h as t wo W A N p o rt s t h at can b e u s ed t o es t ab lis h a co n n ect io n t o t h e in t ern et . Th e fo llo win g ISP co n n ect io n t y p es are s u p p o rt ed : DHCP, St at ic, PPPo E, PPTP, L2TP, 3G In t ern et (v ia USB mo d em).

It is as s u med t h at y o u h av e arran g ed fo r in t ern et s erv ice wit h y o u r In t ern et Serv ice Pro v id er (ISP). By g o in g t h ro ug h a few s t raig ht forward co nfig uratio n p ag es y o u can t ake t h e in fo rmat io n p ro v id ed b y y o ur ISP t o g et y o u r W A N co nnectio n u p an d en ab le in t ern et acces s fo r y o u r n et wo rk. Figure 17 : Inte rne t Conne ction Se tup Wizard Yo u can s t art u sin g t h e W izard b y lo g g ing in wit h t h e ad min is trato r p as s wo rd fo r t h e ro u t er. On ce au t hent icat ed s et t h e t ime zo n e t h at y o u are lo cat ed in , an d t h en ch o o s e t h e t y p e o f ISP co n n ect io n t y p e: DHCP, St at ic, PPPo E, PPTP, L2TP. Us er Name Pas s wo rd Secret (req u ired fo r L2TP o n ly) M PPE En cry p t io n: Fo r PPTP lin ks , y o u r ISP may req u ire y o u t o en able M icro so ft Po in t -t o -Po in t En cry p t io n (M PPE). In s u ch case, u ser h as t o t ake care o f ro u t ing man u ally b y co nfig u ring t he ro u tin g from St at ic Ro u t in g p ag e. co n n ect iv it y Ty pe : To keep t h e co n n ect io n alway s o n , click Keep Co n n ect ed . To lo g o u t aft er t h e co nn ectio n is id le fo r a p erio d o f t ime (u s efu l if y o u r ISP co s t s are b as ed o n lo g o n t imes), click Id le Timeo u t an d en t er t h e t ime, in min u t es , t o wait b efo re d is co n n ect in g in t h e Id le Time field . 2 W AN DNS Serv ers Th e IP A d d res s es o f W A N Do main Name Serv ers (DNS) are t y p ically p ro v id ed d y n amically fro m t h e ISP b u t in s o me cas es y ou can d efin e t h e s tatic IP ad d resses of t h e DNS s erv ers . 39 Unified Services Router User Manual Figure 20 : WAN configurat io n for Japane s e M ultiple PPPoE (part 1) Th ere are a few key elemen t s o f a mu lt ip le PPPo E co n n ect io n : ï□· ï□· Primary an d s eco n d ary co n n ect io n s are co n cu rren t Each s es sio n h as a DNS s erv er s ou rce fo r d o main n ame lo o ku p , t h is can b e assig ned b y t h e ISP o r co n fig u red t h ro u g h t h e GUI ï□· Figure 21 : WAN configurat io n for M ultiple PPPoE (part 2) 3. Th e p rimary an d s eco n d ary DNS s erv ers o n t h e ISPâ□□s IPv 6 n et wo rk are u s ed fo r res o lvin g in t ernet ad d resses, and t h ese are p ro vid ed alo ng wit h t h e s tat ic IPes t raffic t h at is receiv ed o n an y o f it s p h ysical in t erfaces. Bro ad cas t an d mu lt icast p ackets t h at arriv e o n t h e LA N in t erface are s wit ch ed t o t h e W A N an d v ice v ers a, if t h ey d o n o t g et filt ered b y firewall o r VPN p o licies . To main t ain t h e LA N an d W A N in t h e s ame b ro ad cas t d o main s elect Tran s p aren t mo d e , wh ich allo ws b rid g ing o f t raffic fro m LA N t o W A N an d v ice v ers a, excep t fo r ro u t er-t ermin at ed t raffic an d o t h er man ag emen t t raffic . A ll DSR feat u res (su ch as 3G mo d em s u p p o rt) are s u p p o rt ed in t ran s p aren t mo d e as s u min g t h e LA N an d W A N are co n fig u red t o b e in t h e s ame b ro ad cas t d o main . In On ly : Th e ro u t er accept s RIP in fo rmat io n fro m o t h er ro u t ers, b u t d o es not b ro ad cas t it s ro u t in g t ab le.

Th e au t h en t icat io n key v alid it y lifet imes are co n fig u rab le t o en s u re t h at t h e ro u t in g in fo rmat io n exch an g e is wit h cu rren t an d s u p p o rt ed ro u t ers d et ect ed o n t h e LA N. Th e Lis t o f IPv 4 St at ic Ro u t es an d Lis t o f IPv 6 St at ic Ro u t es s h are t h e s ame field s (wit h o n e excep t io n): ï□· A ct iv e: Det ermin es wh et her t h e ro u t e is act iv e o r in act iv e. A ro u t e can b e ad d ed t o t h e t able an d mad e in act ive, if n o t n eeded. Gat eway : IP a d d ress o f t h e g ateway t h ro u g h wh ich t h e d es t in at io n h o s t o r n et wo rk can b e reach ed . Two ro u t ers h av in g a co mmo n s eg men t ; t h eir in t erfaces h av e t o b elo n g t o t h e s ame area o n t h at s eg men t .

If A u t hent icatio n Ty pe is Simp le t h en o s p f p acket s are au t h en t icat ed u s in g s imp le t ext key . ISA TA P s p ecifies an IPv 6-IPv 4 co mp at ib ilit y ad d res s fo rmat as well as a mean s fo r s it e b o rd er ro u t er d is co v ery . ISA TAP als o s p ecifies t h e o p erat io n o f IPv 6 o v er a s p ecific lin k lay er - t h at b ein g IPv 4 u s ed as a lin k lay er fo r IPv 6.

Th ere are a few key elemen t s o f W A N 3 co n fig u rat io n . DNS Serv er So u rce: Ch o o s e o n e o f t h e fo llo win g o p t io n s : o Get Dy n amically fro m ISP: Ch o o s e t his o pt ion if y o u r ISP d id n o t as s ig n a s t at ic DNS IP ad d res s . o Us e Th es e DNS Serv ers : Ch o o se t his o pt ion if y o u r ISP as s ig n ed a s t at ic DNS IP ad d res s fo r y o u t o u s e. A ls o co mp let e t h e field s t h at are h ig h lig h t ed wh it e in t h is s ect io n . Th e W A N M o d e o p t io n s are n o w av ailab le as t h ere are t wo W A N p o rt s fo r t h e g at eway . On ce t he co nnectio n t y pe s et t in g s are co n f ig u red an d s av ed, n avig ate t o t h e W AN s t at us p age (Setup > Internet Settings > WAN 3 Status) an d En ab le t h e W A N3 lin k t o es t ab lis h t h e 3G co n n ect io n . 3.

8 WAN Port Settings Advanced > Advanced Network > WAN Port Setup Th e p h y s ical p o rt s et tin gs fo r each W A N lin k can b e d efin ed h ere. Th is is t h e larg es t p acket s ize t h at can p ass t h roug h t h e in t erface wit h o ut frag men t at io n. Th is s ize can b e in creas ed , h o wev er larg e p ackets can in t rod uce n etwo rk lag an d b rin g d own t h e in t erface s p eed . No t e t h at a 1500 b y t e s ize p acket is t h e larg est allo w ed b y t h e Et h ernet p ro to co l at the n et wo rk lay er. th e p o rt s p eed can b e s en sed b y t h e ro ut er wh en A u to is s elected. W it h t h is o p tion the o p t imal p o rt s et t ing s are d et ermin ed b y t h e ro u t er an d n et wo rk. Th e d u p lex (h alf o r fu ll) can b e d efin ed b ased o n t h e p o rt s up port , as well as o n e o f t h ree p o rt s p eed s : 10 M b p s , 100 M b p s an d 1000 M b p s (i. Th e d efau lt M A C ad d res s is d efin ed d u rin g t h e man u fact u rin g p ro ces s fo r t h e in t erfaces , and can u n iq uely id en tify t h is ro u ter. Yo u can cu st omize each W A N p o rt â□□s M A C ad d res s as n eed ed , eit h er b y let t in g t h e W A N p o rt as s u me t h e cu rren t LA N h o s t â□□s M A C ad d res s o r b y en t erin g a M A C ad d res s man u ally . 11n rad io t h at allo ws y o u t o create an access p oin t for wireles s LA N clien t s .

Th e s ecurit y/ en cry ptio n/ au thent icat io n o p t io n s are g ro u p ed in a wireles s Pro file, an d each co n fig u red p ro file will b e av ailab le fo r s elect io n in t h e A P co n fig u ratio n men u . Th e p ro file d efin es v ario u s p aramet ers fo r t h e A P, in clu d in g t h e s ecu rit y b et ween t h e wireles s clien t an d t h e A P, an d can b e s h ared b et ween mu lt ip le A Ps in s t an ces o n t h e s ame d ev ice wh e n n eed ed . Each s u ch v irt ual A P ap p ears as an in d ep en d en t A P (u n iq u e SSID) t o s u p p o rt ed clien t s in t h e en v iro nmen t, b u t is act ually ru n nin g o n t h e s ame p h ysical rad io in t egrated wit h t h is ro u t er. Ï□□ Pro files may b e t h o u gh t o f as a g ro u pin g o f A P p aramet ers t h at can t h en b e ap p lied t o n o t ju s t o ne b u t mu lt ip le A P in s t ances (SSIDs) , t h u s av o id in g d u p licat io n if t h e s ame p aramet ers are t o b e u s ed o n mu lt ip le A P in s t an ces o r SSIDs . By g o in g t h ro ug h a few s t raig h t fo rward co n fig u rat io n p ag es y o u can en ab le a W i -Fiâ□¢ n et wo rk o n y o u r LA N an d allo w s u p p ort ed 802.
Th is key is t h e p re -s h ared key fo r W PA o r W PA 2 t y p e s ecu rit y . Su p p o rt ed clien t s t h at h av e b een g iv en t his PSK can as s o ciat e wit h t h is A P. Pers onal Identi fi cati on Number (PIN): Th e wireles s d ev ice t h at s u p p o rt s W PS may h av e an alp h an umeric PIN, an d if en t ered in t h is field t h e A P will es t ab lish a lin k t o t h e clien t . Ï□□ Yo u n eed t o en able at leas t o n e A P wit h W PA / WPA 2 s ecu rity an d als o en able W PS in t h e Advanced > Wireless Settings > WPS p ag e t o u s e t h e W PS wizard . The au t h en t icat io n can b e a p re-s h ared key (PSK), En t erp ris e mo d e wit h RA DIUS s erv er, o r b o t h .
W PA 2: t h is s ecu rit y t y p e u s es CCM P en cry p t io n (an d t h e o p t io n t o ad d TKIP en cry p t io n) o n eit h er PSK (p re -s h ared key) o r En t erp ris e (RA DIUS Serv er) au t h en t icat io n . Th is mo d e allo ws leg acy d ev ices t h at o n ly s u p p ort W PA2 key s (s uch as an o ld er wireles s p rin t er) t o co n n ect t o a s ecu re A P wh ere all t h e o t h er wireles s clien t s are u s in g W PA 2. Figure 42 : Lis t of Available Profile s s hows th e options availab le to s e cure the wire le s s link 4. User Manual En cry p t io n : s ele ct t h e en cry p t io n key s ize -- 64 b it W EP o r 128 b it W EP. Th e larg er s ize key s p ro v id e s tron ger en cry pt ion , t h u s makin g t h e key mo re d ifficu lt t o crack ï□· W EP Pas s p hras e: en t er an alp h an u meric p h ras e an d click Gen erat e Key t o g en erat e 4 u n iq u e W EP ke y s wit h len g t h d et ermin ed b y t h e en cry p t io n key s ize. Next c h o o se o n e o f t h e key s t o b e u sed fo r au t henticatio n. 2 W PA or W PA2 with PSK A p re -s h ared key (PSK) is a kn o wn p as sp hrase co nfig u red o n t h e A P an d clien t b o th an d is u s ed t o au t henticate t he wireles s clien t . A s eco n dary RA DIUS s erv er p ro vid es red und an cy in t h e event t hat t h e p rimary s erv er can n o t b e reach ed b y t h e ro u t er wh en n eed ed . Th e Timeo u t an d Ret ries field s are u sed t o eit h er mo v e t o a s econ dary s erver if t h e p rimary can n o t b e reached, o r t o g iv e u p t h e RA DIUS au t h en t icat io n at t emp t if co mmu n icat io n wit h t h e s erv er is n o t p o s s ib le. 74 Unified Services Router User Manual Figure 44 : RADIUS s e rve r (Exte rnal Authe nticatio n) configurat io n 4.

3 Creating and Using Access Points Setup > Wireless Settings > Access Points On ce a p ro file (a g ro u p o f s ecu rity s et tin gs) is created, it can b e as sig ned t o an A P o n t h e ro u t er. Each v irt u al A P t h at h as a u n iq u e SSIDs ap p ears as an in d ep en d en t acces s p o in t t o clien t s . 76 Unified Services Router User Manual Figure 46 : Lis t of configure d acce s s points (Virtu al APs) s hows one e nable d acce s s point on the radio, broadcas t i ng its SSID Th e clien t s co nn ected t o a p art icular A P can b e v iewed b y u s ing t he St atu s Bu t t o n o n t h e Lis t o f A v ailab le A cces s Po in t s . Traffic s t at is t ics are s h o wn fo r t h at in d iv id u al A P, as co mp ared t o t h e s ummary s t ats fo r each A P o n t h e St at ist ics t ab le. Co n n ect ed clien t s are s o rted b y t h e M A C ad d ress an d in d icat e t h e s ecu rit y p aramet ers u s ed b y t h e wireles s lin k, as well as t h e t ime co n n ect ed t o t h is p art icu lar A P.

11n clien t s are exp ect ed t o acces s t he LA N v ia t h is ro u t er, creat in g 3 VA Ps will allo w y o u t o man age o r s h ap e t raffic fo r each g ro up o f clien ts. In t h is way leg acy clien t s can acces s t h e n et wo rk wit h o u t b rin g in g d o wn t h e o v erall t h ro u g h p u t o f mo re cap ab le 802. Sin ce W PA 2 is mo re s ecu re, y o u may wan t t o b ro ad cas t t h is SSID an d n o t 77 Unified Services Router User Manual b ro ad cast t h e SSID fo r t h e VA P wit h W EP s in ce it is mean t t o b e u s ed fo r a few leg acy d ev ices in t h is s cen ario . Figure 47 : Radio card configurat io n options Th e rat ified 802. Fo r examp le, ch an g in g t h e ch an n el s p acin g t o 40 M Hz can imp ro v e b an d wid t h at t h e exp en s e o f s u p p o rt in g earlier 802. 11n clien t s . Th e av ailab le t ran smis sio n ch ann els are g o v ern ed b y reg u latory co nst rain t s b as ed o n t h e reg io n s et t in g o f t h e ro u t er. Figure 48 : Wi-Fi M ultime dia Profi l e Name : Th is field allo ws y o u t o s elect t h e a v ailab le p ro files in wireles s s et t in g s . enabl e WMM: Th is field allo ws y o u t o en ab le W M M t o imp ro v e mu lt imed ia t ran s mis s io n . Defaul t Cl as s Of S ervi ce : Th is field allo ws y o u t o s elect t h e av ailab le A cces s Cat eg o ries (v o ice, v id eo , b es t effo rt , an d b ackg ro u n d). Th e in p u t s t o t his fu nctio n are a PSK (co n fig u rab le b y an ad mi n is t rat o r fro m t h e W DS p ag e) an d an in t ern al " mag ic" s t rin g (n o n -co n fig u rab le). In effect t h e W DS lin ks u s e TKIP/ A ES en cry p t io n , d ep en d in g o n t h e en cry p t io n co n fig u red fo r t h e d efault A P. WDS Enabl e - Th is wo u ld b e a ch eck b o x W DS En cry p t io n - Dis p lay s t he t y pe o f en crypt ion u s ed . Th is field in t h e W DS Co n fig u rat io n s ectio n d is p lay s t h e d ev ice's mac ad d res s, wh ich n eeds t o b e s pecified o n t h e W DS p eer fo r makin g a co n n ect ion t o t h is d ev ice (Similarly t h e W DS p eers M A C ad d res s will h av e t o b e s p ecified o n t h is d ev ice fo r t h e W DS lin k t o b e es t ab lis h ed b et ween t h e t wo d ev ices). Pers onal Identi fi cati on Number (PIN): Th e wireles s d ev ice t h at s u p p o rt s W PS may h av e an alp h an u meric PIN, if s o ad d t h e PIN in t h is field . 82 Unified Services Router User Manual ï□□ M o re t h an o n e A P can u s e W PS, b u t o n ly o n e A P can b e u s ed t o es t ab lis h W PS lin ks t o clien t at an y g iv en t ime. Figure 51 : WPS configurat io n for an AP with WPA/WP A2 profile 83 Chapter 5. Securing the Private Network Yo u can s ecu re y ou r n etwo rk b y creat in g an d ap p ly in g ru les t h at y o u r ro u t er u s es t o s elect iv ely b lo ck an d allo w in b o u n d an d o u t b o u n d In t ern et t raffic. Rep o rt s an d alert s t h at y o u wan t t h e ro u t er t o s en d t o y o u Yo u can , fo r examp le, es t ab lis h res t rict ed -acces s p o licies b as ed o n t ime -o f-d ay , web ad d res ses, an d web ad d ress key wo rd s . Â□□ Ho w y o u make y o u r ad d res s kn o wn d ep en d s o n h o w t h e W A N p o rt s are co n fig u red ; fo r t h is ro u t er y o u Unified Services Router User Manual may u s e t h e IP ad d res s if a s t at ic ad d res s is as s ig n ed t o t h e W A N p o rt , o r if y o u r W A N ad d res s is d y n amic a DDNS (Dy n a mic DNS) n ame can b e u s ed . W h en t h e d efau lt o u t b o u n d p o licy is allo w alway s , y o u can t o b lo ck h o s t s o n t h e LA N fro m acces s in g in t ern et s erv ices b y creat in g an o u t b o u n d firewall ru le fo r each s erv ice. figure 52 : Lis t of Available Fire wal l Rule s 5. 2 Defining Rule Schedules Tools > Sche dules Firewall ru les can b e en abled o r d is ab led au t o mat ically if t h ey are as s o ciat ed wit h a co n fig u red s chedule. 3 Configuring Firewall Rules Advanced > Firewall Settings > Firewall Rules A ll co n fig u red firewall ru les o n t h e ro u t er are d is p lay ed in t h e Firewall Ru les lis t . View the existing rules in the List of Available Firewall Rules table.

2. To edit or add an outbound or inbound services rule, do the following: ï□· Chose the From Zone to be the source of originating traffic: either the secure LAN, public DMZ, or insecure WAN. For an inbound rule WAN should be selected as the From Zone. 4. Choose the To Zone to be the destination of traffic covered by this rule. If the From Zone is the WAN, the to Zone can be the public DMZ or secure LAN. Similarly if the From Zone is the LAN, then the To Zone can be the public DMZ or insecure WAN. 5. Parameters that define the firewall rule include the following: 87 Unified Services Router ï□· User Manual Serv ice : A NY mean s all t raffic is affect ed b y t h is ru le. Fo r a s p ecific s erv ice t h e d ro p d o wn lis t h as co mmo n s erv ices , o r y o u can s elect a cu s t o m d efin ed s erv ice.

Ï□§ So u rce & Des t in at io n u sers: Fo r each relev an t cat ego ry, s elect t he u sers t o wh ich t h e ru le ap p lies : ï□· Inbound rules can use Destination NAT (DNAT) for managing traffic from the WAN. Ï□§ Yo u can en ab le p o rt fo rward in g fo r an in co min g s erv ice s p ecific ru le (Fro m Zo n e = W A N) b y s elect in g t h e ap p ro p riat e ch eckb o x. Th is will allo w t h e s elect ed s erv ice t raffic fro m t h e in t ern et t o reach t h e ap p ro p riat e LA N p o rt v ia a p o rt fo rward in g ru le. If y o u r ISP as s ig ns y o u mo re t h an o n e p u b lic IP ad d res s , o n e o f t h es e can b e u s ed as y o u r p rimary IP ad d res s o n t h e W A N p o rt , an d t h e o t h ers can b e assig ned t o s erv ers o n t h e LA N o r DM Z. In t h is way t h e LA N/ DM Z s erv er can b e acces s ed fro m t h e in t ern et b y it s alias ed p u b lic IP ad d res s .

7. Outbound rules can use Source NAT (SNAT) in order to map (bind) all LAN/DMZ traffic matching the rule parameters to a specific WAN interface or external IP address (usually provided by your ISP). On ce t h e n ew o r mo d ified ru le p aramet ers are s av ed , it ap p ears in t h e mas t er lis t o f firewall ru les . 89 Unified Services Router User Manual Figure 54 : Example whe re an outbound SNAT rule is us e d to map an e xte rnal IP addre s s (209. 30) 90 Unified Services Router User Manual Figure 55 : The fire wal l rule configuratio n page allows you to de fine the To/From zone , s e rvice , action, s che dule s , and s pe cify s ource /de s tination IP addre s s e s as ne e de d.

91 Unified Services Router User Manual 5. 4 Configuring IPv6 Firewall Rules Advanced > Firewall Settings > IPv6 Firewall Rules A ll co n fig u red IPv 6 firewall ru les o n t h e ro u t er are d is p lay ed in t h e Firewall Ru les lis t . th is lis t als o in d icat es wh et h er t h e ru le is en ab led (act iv e) o r n o t , an d g iv es a s u mmary o f t h e Fro m/ To zo n e as well as t h e s erv ices o r u s ers t h at t h e ru le affect s .

Figure 56 : The IPv6 fire wall rule configuratio n page allows you to de fine the To/From zone , s e rvice , action, s che dule s , and s pe cify s ource /de s tination IP addre s s e s as ne e de d. In t h e examp le, CUSeeM e (t h e v id eo co n feren ce s erv ice u s ed) co n n ect io n s are allo wed o n ly fro m a s p ecified ran g e o f ext ern al IP ad d res s es . If y o u arran g e wit h y o u r ISP t o h av e mo re t h an o ne p u blic IP ad d ress fo r y o u r u se, y ou can u s e t h e ad dit io nal p u blic IP ad d resses t o map t o s erv ers o n y o u r LA N. Th e o t her ad dress es are av ailab le t o map t o y o u r DM Z s erv ers . Since we are trying to block HTTP requests, it is a service with To Zone: Insecure (WAN1/WAN2/WAN3) that is to be blocked according to schedule â□□Weekendâ□□. 96 Unified Services Router User Manual 3. Select the Action to â□□Block by Schedule, otherwise allowâ□□.

This will take a predefined schedule and make sure the rule is a blocking rule during the defined dates/times. All other times outside the schedule will not be affected by this firewall blocking rule 4. As we defined our schedule in schedule â□□Weekendâ□□, this is available in the dropdown menu 5. We want to block the IP range assigned to the marketing group. Letâ□□s say they have IP 192. On the Source Users dropdown, select Address Range and add this IP range as the from and To IP addresses. 6. We want to block all HTTP traffic to any services going to the insecure zone. We donâ□□t need to change default QoS priority or Logging (unless desired) â□□ clicking apply will add this firewall rule to the list of firewall rules . 8.
The last step is to enable this firewall rule. Select the rule, and click â□□enableâ□□ below the list to make sure the firewall rule is active 5. In t h e cu s t om s erv ice co nfig uratio n men u y o u can d efin e a ran g e o f p o rt s an d id en t ify t h e t raffic t y p e (TCP/ UDP/ ICM P) fo r t h is s erv ice. On ce d efin ed , t h e n ew s erv ice will ap p ear in t h e s erv ices lis t o f t h e firewall ru les co n fig u rat io n men u . 97 Unified Services Router User Manual Figure 59 : Lis t of us e r de fine d s e rvice s .
Figure 60 : Cus tom Se rvice s configuratio n Creat ed s erv ices are av ailab le as o p t io n s fo r firewall ru le co n fig u rat io n . name: Name o f t h e s erv ice fo r id en t ificat io n an d man ag emen t p u rp o s es . Ty p e: Th e lay er 3 Pro t o co l t h at t h e s erv ice u s es . (TCP, UDP, BOTH, ICM P o r ICM Pv 6) Po rt Ty p e: Th is field s allo ws t o s elect Po rt Ran g e o r M u lt ip le Po rt s ICM P Ty p e: Th is field is en ab led wh en t h e lay er 3 p ro t o co l (in t h e Ty p e field) is s elect ed as ICM P o r ICM Pv 6. 6 ALG support Advanced > Firewall Settings > ALGs A p p licat io n Lev el Gat eway s (A LGs) are s ecu rit y co mp o nent t hat en h ance t h e firewall an d NA T s u p p ort o f t h is ro u ter t o s eamles sly s up p o rt ap p licat io n lay er p ro t o co ls .
7 VPN Passthrough for Firewall Advanced > Firewall Settings > VPN Passthrough Th is ro u t erâ□□s firewall s et t in g s can b e co n fig u red t o allo w en cry p t ed VPN t raffic fo r IPs ec , PPTP, an d L2TP VPN t u n n el co n n ect io n s b et ween t h e LA N an d in t ern et . a s p ecific firewall ru le o r s erv ice is n o t ap p ro p riat e t o in t ro d u ce t h is p as s t h ro u g h s u p p ort ; in s tead t he ap p ro p riat e ch eck b o xes in t h e VPN Pas s t h ro u g h p ag e mu s t b e en ab led . 100 Unified Services Router User Manual Figure 62 : Pas s through options for VPN tunne ls 5. A s well p o rt s are n o t left o p en wh en n o t in u s e, t h ereby p ro vid in g a lev el o f s ecu rit y t h at p o rt fo rward in g d o es n o t o ffer. Ï□□ Po rt t rig g erin g is n o t ap p ro p riat e fo r s erv ers o n t h e LA N, s in ce t h ere is a d ep en d en cy o n t h e LA N d ev ice makin g an o u t g o in g co n n ect io n b ef o re in co min g p o rt s are o p en ed . 101 Unified Services Router User Manual Figure 63 : Lis t of Available Applicat io n Rule s s howing 4 unique rule s Th e ap p licat io n ru le s t atus p age will lis t an y act iv e ru les , i. Pro xy s erv ers , wh ich can b e u s ed t o circu mv en t cert ain firewall ru les an d t h u s a p o t en t ial s ecu rit y g ap , can b e b lo cked fo r all LA N d ev ice s . Jav a ap p let s can b e p rev en t ed fro m b ein g d o wn lo ad ed fro m in t ern et s it es , an d s imilarly t h e g at eway can p rev en t A ct iv eX co n t ro ls fro m b ein g d o wn lo aded v ia In t ernet Exp lo rer. Fo r ad d ed s ecu rit y co o kies , wh ich t y p ically co n t ain s es s io n in fo rmat io n , can b e b lo cked as well fo r all d ev ices o n t h e p riv at e n et wo rk. 102 Unified Services Router User Manual Figure 64 : Conte nt Filte ring us e d to block acce s s to proxy s e rve rs and pre ve nt Active X controls from be ing downloade d 5.

Fo r examp le, if t h e d o main â□□y ah o o â□□ is ad d ed t o t h is lis t t h en all o f t h e fo llo win g URLâ□□s are p ermit t ed acces s fro m t h e LA N: www. Exp o rt Blo cked Key wo rd s : Th is feat ure en ab les t he u ser t o exp o rt t he key wo rds t o b e b lo cked t o a cs v file wh ich can t h en b e d o wn loaded t o t h e lo cal h o st. Th is is IP/ M A C Bin d in g , an d b y en fo rcin g t h e g ateway t o v alid ate t h e s ou rce t rafficâ□□s IP ad d res s wit h t h e u n iq u e M A C A d d res s o f t h e co n fig u red LA N n o d e , t h e ad min is t rat o r can en sure t raffic fro m t h at IP ad d res s is n ot s poo fed . T h e t rafficâ□□s s ou rce IP ad d ress d oesnâ□□t mat ch u p wit h t h e exp ect ed MAC ad d res s h avin g t h e s ame IP ad d ress) t h e p ackets will b e d ro p p ed an d can b e lo g ged for d iag n o s is . 106 Unified Services Router User Manual Figure 68 : The followi ng e xample binds a LAN hos tâ□□s M AC Addre s s to an IP addre s s s e rve d by DSR. If the re is an IP/M AC B inding violation, the violating pack e t will be droppe d and logs will be capture d 5. Th e ch ecks can b e en ab led b et ween t h e W A N an d DM Z o r LA N, an d a ru n n in g co u n t er w ill allo w t h e ad min is t rat o r t o see h ow man y malicio u s in t ru sio n at temp t s fro m t h e W A N h av e b een d et ect ed an d p rev en t ed . 12 Protecting from Internet Attacks Advanced > Advanced Network > Attack Checks A t t acks can b e malicio u s s ecu rit y b reach es o r u n in t en t io n al n et wo rk is s u es t h at ren d er t h e ro u t er u n u s ab le. A t t ack ch ecks allo w y o u t o man ag e W A N s ecu rit y t h reat s s uch a s co ntin ual p in g req uests an d d is co very v ia A RP s can s . tCP an d UDP flo o d at t ack ch ecks can b e en ab led t o man ag e ext reme u s ag e o f W A N res o u rces .

A d d it io n ally cert ain Den ial-o f-Serv ice (Do S) at t acks can b e b lo cked. 108 Unified Services Router User Manual Figure 70 : Prote cting the route r and LAN from inte rne t attack s WAN S ecuri ty Check s : En ab le St ealt h M o d e: If St ealt h M o de is en ab led, t h e ro u ter will n o t res p ond t o p o rt s can s fro m t h e W A N. UDP Co n n ect io n Limit : Yo u can s et t h e n u mb er o f s imu lt an eo u s act iv e UDP co n n ect io n s t o b e accep t ed fro m a s in g le co mp u t er o n t h e LA N; t h e d efau lt is 25 ICS A S etti ng s : Blo ck ICM P No t ificat io n : s elect in g t h is p rev en t s ICM P p acket s fro m b ein g id en t ified as s uch. Th e fo llo win g t y p es o f t u n n els can b e creat ed : ï· Figure 71 : Example of Gate way-to - Gate way IPs e c VPN tunne l us ing two DSR route rs conne cte d to the Inte rne t 111 Unified Services Router User Manual Figure 72 : Example of thre e IPs e c clie nt conne ctions to the inte rnal ne twork through the DSR IPs e c gate way 112 Unified Services Router User Manual 6. Select the VPN tunnel type to create ï· Set t h e Co n n ect io n Name an d p re -s h ared key : t h e co n n ect io n n ame is u s ed fo r man ag emen t , an d t h e p re -sh ared key will b e req u ired o n t h e VPN clien t o r g at eway t o es t ab lis h t h e t u n n el ï· Configure Remote and Local WAN address for the tunnel endpoints ï· remo t e Gat eway Ty p e: id en t ify t h e remo t e en d p o in t o f t h e t u n n el b y FQDN o r s t at ic IP ad d res s ï· Remo t e W A N IP ad d res s / FQDN: Th is field is en ab led o n ly if t h e p eer y o u are t ry in g t o co n n ect t o is a Gat eway .

Lo cal W A N IP ad d ress / FQDN: Th is field can b e left b lan k if y o u are n o t u s in g a d ifferen t FQDN o r IP ad d res s t h an t h e o n e s p ecified in t h e W A N p o rt â□□s co n fig u rat io n . 3. Configure the Secure Connection Remote Accessibility fields to identify the remote network: ï· Review the settings and click Connect to establish the tunnel. Th e W izard will creat e an A u t o IPs ec p o licy wit h t h e fo llo win g d efau lt v alu es fo r a VPN Clien t o r Gat eway p o licy (t h es e can b e acces s ed fro m a lin k o n t h e W izard p ag e): Par am eter Exchange Mode ID Type Local WAN ID Remote WAN ID Encryption Algorithm Authentication Algorithm Authentication Method PFS Key-Group Life Time (Phase 1) Life Time (Phase 2) De f au lt value f rom Wizard Aggressive (Client policy) or Main (Gatew ay policy) FQDN w an_local. On ce t h e W izard creat es t h e mat ch in g IKE an d VPN p o licies req u ired b y t h e A u t o p o licy , o n e can mo d ify t h e req uired field s t h ro ugh t he ed it lin k.

On ly t h e d at a p ay lo ad is en cry pted an d t he IP h ead er is n o t mo d ified o r en cry p t ed . A s well in t h is mo d e y o u can d efin e t h e s ing le IP ad d ress, ran ge o f IPs , o r s u b net o n b oth t h e lo cal an d remo t e p riv at e n et wo rks t h at can co mmu n icat e o v er t h e t u n n el. 115 Unified Services Router User Manual Figure 74 : IPs e c policy configurat ion On ce t h e t u n nel t y p e an d en d poin t s o f t h e t u n n el are d efin ed y o u can d et ermin e t h e Ph as e 1 / Ph as e 2 n eg o t iatio n t o u se fo r t h e t un nel. Th e Ph as e 2 A u t o p o licy p aramet ers co v er t h e s ecu rit y as s o ciat io n lifet ime an d en cry p t io n / a u t h en t icat io n d et ails o f t h e p h as e 2 key n eg o t iat io n . 116 Unified Services Router User Manual Th e VPN p o licy is o n e h alf o f t h e IKE/ VPN p o licy p air req u ired t o est ab lis h an A u t o IPs ec VPN t u n n el. Th e IP ad d res s es o f t h e mach in e o r mach in es o n t h e t wo VPN en d p o in ts are co nfig u red h ere, alo n g wit h t h e p o licy p aramet ers req u ired t o s ecure t he t u n n el Figure 75 : IPs e c policy configurat ion continue d (Auto policy via IKE) A M an u al p o licy d o es n ot u s e IKE an d in s t ead relies o n man u al key in g t o exch an g e au t h en ticat io n p aramet ers b etween t h e t wo IPs ec h o s t s . th e in co min g an d o u t g o in g s ecu rit y p aramet er in d ex (SPI) v alu es mu s t b e mirro red o n t h e remo t e t u n n el 117 Unified Services Router User Manual en d p o in t. A s well t h e en cry pt io n an d in t egrit y alg o rit hms an d key s mu s t mat ch on the remo t e IPs ec h o s t exact ly in o rd er fo r t h e t u nn el t o es t ab lis h s u cces s fu lly . No t e t h at u s in g A u to p olicies wit h IKE are p referred as in s o me IPs ec imp lemen t at io n s t h e SPI (s ecu rit y p aramet er in d ex) v alu e s req u ire co n v ers io n at each en d p o in t . Rat h er t h an co n fig u re a u n iq u e VPN p o licy fo r each u s er, y o u can co n fig u re t h e VPN g at eway ro u t er t o au t h en t icat e u s ers fro m a s t o red lis t o f u s er acco u n t s o r wit h an ext ern al au t h en ticat io n s erv er s u ch as a RA DIUS s erv er.

Fo r RA DIUS â□□ PA P, t h e ro u t er firs t ch ecks in t h e u ser d atabase t o s ee if t h e u s er cred en t ials are av ailab le; if t h ey are n o t , t h e ro u t er co n n ect s t o t h e RA DIUS s erv er. 3 Configuring VPN clients Remo t e VPN clien t s mu s t b e co nfig u red wit h t h e s ame VPN p o licy p aramet ers used in t h e VPN t u n n el t h at t h e clien t wis h es t o u se: en crypt io n, au thent icat ion , life t ime, an d PFS key -g ro u p . Op en so urce s o ftware (s uch as Op en VPN o r Op en s wan) as well as M icro s o ft IPs ec VPN s o ft ware can b e co n fig u red wit h t h e req u ired IKE p o licy p aramet ers t o est ab lish an IPs ec VPN t u n n el. Th e ro u t er act s as a b ro ker d ev ice t o allo w t h e ISP's s erv er t o creat e a TCP co n t ro l co n n ect io n b et ween t h e LA N VPN clien t an d t h e VPN s erv er. On ce t h e PPTP s erv er is en ab led , PPTP clien t s t h at are wit h in t h e ran g e o f co n fig u red IP ad d re s ses o f allo wed clien t s can reach t he ro u terâ□□s PPTP s erv er. On ce t h e L2TP s erv er is en ab led , L2TP clien t s t h at are wit h in t h e ran g e o f co n fig u red IP ad d res ses o f allo wed clien t s can reach t he ro u terâ□□s L2TP s erv er. 3 OpenVPN Support Setup > VPN Settings > OpenVPN > OpenVPN Configuration Op en VPN allo ws p eers t o au t h en t icat e each o t h er u s in g a p re -s h ared s ecret key , cert ificat es , o r u sername/ passwo rd . En cry p t io n A lg orit hm: Th e cip h er wit h wh ich t h e p ackets are en cry pt ed . Can b e ch ecked o n ly wh en t h e t ls key is u p lo ad ed . Th e ro u t er s u p p o rt s mu lt ip le co n cu rren t s es s io n s t o allo w remo t e u s ers t o acces s t h e LA N o v er an en cry p t ed lin k t h ro u g h a cu s t o mizab le u s er p o rt al in t erface, an d each SSL VPN u s er can b e as s ig n ed u n iq u e p riv ileg es an d n et wo rk res o u rce acces s lev els .

Th e remo t e u s er can b e p ro vid ed d ifferent o pt io ns fo r SSL s erv ice t h ro u g h t h is ro u t er: ï□· On ce es t ab lis h ed , t h e h o s t mach in e can acces s allo cat ed n et wo rk res o u rces . Th e ro ut er ad min is t rat or can d efine s pecific s erv ices o r ap p licatio ns t h at are av ailable t o remo t e p o rt fo rward in g u s ers in s t ead o f acces s t o t h e fu ll LA N like t h e VPN t u n n el. Figure 85 : Lis t of groups Gro u p co n fig u rat io n p age allo ws t o creat e a g ro u p wit h a d ifferen t t y pe o f u s ers . PPTP Us er: Th es e are PPTP VPN t u n n el LA N u s ers t h at can es tablis h a t unnel wit h t h e PPTP s erv er o n t h e W A N. L2TP Us er: Th es e are L2TP VPN t u n n el LA N u s ers t h at can es tablis h a t unnel wit h t h e L2TP s erv er o n t h e W A N.

Figure 86 : Us e r group configu rat ion W h en SSLVPN u s ers are s elect ed , t h e SSLVPN s et t in g s are d is p lay ed wit h t h e fo llo win g p aramet ers as cap t u red in SSLVPN Set t in g s . If t h ere are mu lt ip le wo rkg ro u p s , u s er can en t er t h e d et ails fo r u p t o t wo wo rkg ro u p s . lDA P Bas e DN: Th is is t h e b as e d o main n ame fo r t h e LDA P au t h en t icat io n s erv er. If t h ere are mu lt ip le LDA P au t h en ticatio n s erv ers , u s er can en t er t h e d et ails fo r u p t o t wo LDA P Bas e DN. If t h ere are mu lt ip le A ct iv e Direct o ry d o main s , u s er can en t er t h e d et ails fo r u p t o t wo au t h en t icat io n d o main s .

Th e fo llo win g p aramet ers are co n fig u red : ï□· User Manual Dis ab le Lo g in : En ab le t o p rev en t t h e u sers o f t h is g ro up fro m lo g g in g in t o the d ev ices man ag emen t in t erface(s) Den y Lo g in fro m W A N in t erface: En ab le t o p rev en t t h e u s ers o f t h is g ro u p fro m lo g g in g in fro m a W A N (wid e area n et wo rk) in t erface. Th e fo llo win g p aramet ers are co n fig u red : ï□· Defin ed Bro ws ers :Th is lis t d is plays t h e web b ro ws ers t h at h ave b een add ed t o t h e Defin ed Bro ws ers lis t , u p o n wh ich g ro u p lo g in p o licies can b e d efin ed . Yo u can ad d t o t h e lis t o f Defin ed Bro ws ers b y s elect ing a clien t b ro wser fro m the d ro p d o wn men u an d clickin g A d d. Th e fo llo win g p aramet ers are co n fig u red : ï□· Defin ed Bro ws ers :Th is lis t d is plays t h e web b ro ws ers t h at h ave b een add ed t o t h e Defin ed Bro ws ers lis t , u p o n wh ich g ro u p lo g in p o licies can b e d efin ed . Yo u can ad d t o t h e lis t o f Defin ed Bro ws ers b y s elect ing a clien t b ro wser fro m the d ro p d o wn men u an d clickin g A d d. Th e lis t s o f av ailable u sers are d is played in t h e â□□Lis t o f Us ers â□□ p ag e wit h Us er n ame, as s o ciat ed g ro u p an d Lo g in s t at u s . Click Delet e t o clear an exis t in g u s er 136 Unified Services Router User Manual Figure 91 : Available Us e rs with login s tatus and as s ociate d Group 7. Th e u s er s et t in g s co n t ain t h e fo llo win g key co mp o n en t s : ï□· Th e Lis t o f A v ailab le Po licies can b e filt ered b as ed o n wh et h er it ap p lies t o a u s er, g ro u p , o r all u s ers (g lo b al). Bas ed o n t h e s elect io n o f o n e o f t h es e fo u r o p t io n s , t h e ap p ro p riat e co n fig u ratio n field s are req u ired (i. A s well t h e p o licy can b e sp ecified for o n e o r all o f t h e s u p p o rt ed SSL VPN s erv ices (i.

Th e p o licy n ame, SSL s erv ice it ap p lies t o , d es t in at io n (n et wo rk res o u rce o r IP ad d res s es) an d p ermis s io n (d en y / p ermit) is o u t lin ed in a lis t o f co n fig u red p o licies fo r t h e ro u t er. Net wo rk res o u rces are creat ed wit h t h e fo llo win g in fo rmat io n Permis s io n : Th e as sig n ed res o u rces d efin ed b y t h is p o licy can b e exp licit ly p ermit t ed o r d en ied . 1 Using Network Resources Setup > VPN Settings > SSL VPN Server > Resources Net wo rk res o u rces are s erv ices o r g ro u p s o f LA N IP ad d res s es t h at are u s ed t o eas ily creat e an d co n fig u re SSL VPN p o licies . A n et wo rk res o u rce can b e d efin ed b y co n fig u rin g t h e fo llo win g in t h e GUI: ï□· Th e t able b elo w lis t s s o me co mmo n ap p licat io n s an d co rres p o n d in g TCP p o rt n u mb ers : T CP Ap p lication FTP Data (usually not needed) FTP Control Protocol SSH Telnet SMTP (send mail) HTTP (w eb) POP3 (receive mail) NTP (netw ork time protocol) Citrix Terminal Services VNC (virtual netw ork computing) Po r t Num ber 20 21 22 23 25 80 110 123 1494 3389 5900 or 5800 142 Unified Services Router User Manual A s a co n v enien ce fo r remo t e u s ers , t h e h o s t n ame (FQDN) o f t h e n et wo rk s erv er can b e co n fig u red t o allo w fo r IP ad d ress res olu tio n . th is h o s t n ame res o lu t io n p ro v id es u s ers wit h eas y -t o -rememb er FQDNâ□□s t o acces s TCP ap p licat io n s in s t ead o f erro r p ro n e IP ad d res s es wh en u s in g t h e Po rt Fo rward in g s erv ice t h ro u g h t h e SSL Us er Po rt al. To co n fig u re p o rt fo rward in g , fo llo win g are req u ired : ï□· Allo w u s ers t o access t he p riv ate n et work s erv ers b y u sin g a h o st name in s tead o f an IP ad d res s, t he FQDN co rres p on din g t o t he IP ad d ress is d efin ed in t h e p o rt fo rward in g h o s t co n fig u rat io n s ect io n . Th es e clien t ro u t es g iv e t h e SSL clien t access t o s pecific p riv at e n et works , t hereby allo win g access co n t ro l o v er s p ecific LA N s erv ices . clien t lev el co n fig u rat io n s u p p o rt s t h e fo llo win g : ï□· En ab le Sp lit Tu n n el Su p p o rt : W it h a s p lit t u n n el, o n ly res o u rces wh ich are referen ced b y clien t ro u t es can b e acces s ed o v er t h e VPN t u n n el. W it h fu ll t u n n el s u p p o rt (if t h e s p lit t u n n el o p t io n is d is ab led t h e DSR act s in fu ll t u n n el mo d e) all ad d res s es o n t h e p riv at e n et wo rk are acces s ib le o v er t h e VPN t u n n el. A s well a s t at ic ro u t e o n t h e p riv at e LA Nâ□□s firewall (t y p ically t h is ro u ter) is n eed ed t o fo rward p riv ate t raffic t h rou gh t h e VPN Firewall t o t h e remo t e SSL VPN clien t .

Figure 98 : Configu re d clie nt route s only apply in s plit tunne l mode ï□□ ï□□ ï□□ ï□□ S teps to Ins tal l / Uni ns tal l S S LVPN tunnel i n MA C OS 1. The configure d portal can the n be as s ociate d with an authe ntic at io n domain 7. Th ere are v ario u s field s in t h e p o rt al t h at are cu s t o mizab le fo r t h e d o main , an d t h is a llo ws t h e ro u t er ad min is t rat o r t o co mmu n icat e d et ails s uch as lo g in in s tructio ns, av ailable s erv ices , an d o t h er u s ag e d et ails in t h e p o rt al v is ib le t o remo t e u sers.

Du rin g d o main s etup , co n fig u red p o rt al lay o u t s are av ailab le t o s elect fo r all u s ers au t h en t icat ed b y t h e d o main . A s well, t h e u s ers as s ig n ed t o t h is p o rt al (t h ro u g h t h eir au t h en ticat io n d o main) can b e p resent ed wit h o n e o r mo re o f t h e ro u t erâ□□s s u p p o rt ed SSL s erv ices s u ch as t h e VPN Tu n n el p ag e o r Po rt Fo rwa rd in g p ag e.

To co n fig u re a p o rt al lay o u t an d t h eme, fo llo win g in fo rmat io n is n eed ed : ï□· Po rt al s it e t it le: Th e p o rt al web b ro ws er win d o w t it le t h at ap p ears wh en t h e clien t acces s es t h is p o rt al. Dis p lay b an n er mes s ag e o n t h e lo g in p age: Th e u s er h as t h e o p t io n t o eit h er d is p lay o r h id e t h e b an n er mes s ag e in t h e lo g in p ag e. A ct iv eX web cach e clean er: A n A ct iv eX cach e co n t ro l web clean er can b e p u s h ed fro m t h e g at eway t o t h e clien t b ro ws er wh en ev er u s ers lo g in t o t h is SSL VPN p o rt al. SSL VPN p o rt al p ag e t o d is play : Th e Us er can eit h er en able VPN t u n n el p ag e o r Po rt Fo rward in g , o r b o t h d epend ing o n t h e SSL s erv ices t o d is p lay o n t h is p o rt al. On ce t h e p o rt al s ettin gs are co n fig u red , t h e n ewly co n fig u red p o r t al is ad d ed t o t h e lis t o f p o rt al lay o u t s .

USB M as s St o rag e: als o referred t o as a â□□s h are p o rt â□□, files o n a USB d is k co n n ect ed t o t h e DSR can b e acces s ed b y LA N u s ers as a n et wo rk d riv e. Select t h e 'Co n n ect t o p rin ter u sin g URL' rad io b u t t o n ('Select a s hared p rin t er b y n ame â□□in cas e o f W in d o ws 7) an d g iv e t h e fo llo win g URL h t t p :// <Ro u t er's LA N IP ad d res s>:631/ p rin ters / <M o d el Name> (M o d el Name can b e fo u n d in t h e USB s t at u s p ag e o f ro u t er's GUI). Th e USB p rin t er can b e acces s ed o n an y LA N h o s t (wit h ap p ro p riat e p rin t er d riv er in s t alled) co n nected t o t h e ro u t er b y u s in g t h e fo llo win g co mman d in t h e h o s t 's ad d p rin t ers win d o w h t t p ://<Ro uter's IP:631>/ p rin t ers/ <Device M od el> (Dev ice M o d el can b e fo u n d in t h e USB s et t in g s p ag e). Th e USB p rin t er can b e acces s ed o n an y LA N h o s t (wit h ap p ro p riat e p rin t er d riv er in s t alled) co n nected t o t h e ro u t er b y u s in g t h e fo llo win g co mman d in t h e h o s t 's ad d p rin t ers win d o w h t t p ://<Ro uter's IP:631>/ p rin t ers/ <Device M od el> (Dev ice M o d el can b e fo u n d in t h e USB s et t in g s p ag e). Th e receiv ed mes s ag es can b e s een in t h e In b o x a n d allo ws t h e u ser t o create a n ew SM S. if W A N3 is u s ed in d ed icat ed wan mo d e , lo ad b alan cin g mo d e o r if 3G USB Dev ice is n o t co n n ect ed t o ro u t er t h en t h e co n t ro ls o n t h is p ag e will b e g rey ed o u t . Figure 103 : SM S Se rvice â□□ Se nd SM S Th e fo llo win g d et ails are d is p lay ed in SM S INBOX p ag e: ï□· TimeSt amp : Dis p lay s t h e t ime wh en t h e mes s ag e was s en t Text : Dis p lay s t h e co n t en t o f t h e p art icu lar M es s ag e. Th e fo llo win g act io n s are p erfo rmed : Delet e : Delet es t h e SM S h av in g t h at p art icu lar Sn o . Th e fo llo win g cert ificat e d at a is d is p lay ed in t h e lis t o f Tru s t ed (CA) cert ificat es : CA Id en t it y (Su b ject Name): Th e cert ificat e is is s u ed t o t h is p ers o n o r o rg an izat io n Is s u er Name: Th is is t h e CA n ame t h at is s u ed t h is cert ificat e Exp iry Time: Th e d at e aft er wh ich t h is Tru s t ed cert ificat e b eco mes in v alid A s elf cert ificat e is a cert ificat e is s u ed b y a CA id en t ify in g y o u r d ev ice (o r s elf s ig n ed if y o u d o nâ□□t wan t t h e id ent ity p ro tect ion o f a CA). th e A ct iv e Self Cert ificat e 154 Unified Services Router User Manual t ab le lis t s t h e s elf cert ificat es cu rren t ly lo ad ed o n t h e g at eway .

Th e fo llo win g in fo rmat io n is d is p lay ed fo r each u p lo ad ed s elf cert ificat e: ï□· Th is s ho uld b e y ou r o fficial reg is t ered o r co mp an y n ame, as IPs ec o r SSL VPN p eers are s h o wn t h is field . To req u es t a s elf cert ificat e t o b e s ig n ed b y a CA , y o u can g en erat e a Cert ificat e Sig n in g Req u est fro m t h e g at eway b y ent erin g id ent ificatio n p aramet ers an d p ass ing it alo n g t o t h e CA fo r s ig n in g . On ce s ig n ed , t h e CA â□□s Tru s t ed Cert ificat e an d s ig n ed cert ificat e fro m t h e CA are u p lo ad ed t o act iv at e t h e s elf-cert ificat e v alid at in g t h e id en t it y o f t h is g at eway . th e s elf cert ificat e is t h en u s ed in IPs ec an d SSL co n n ect io n s wit h p eers t o v alid at e t h e g at eway â□□s au t h en t icit y . Figure 105 : Ce rtificate s ummary for IPs e c and HTTPS manage me nt 155 Unified Services Router User Manual 8. Th e ro u t er ad min is t rat o r can d efin e a kn o wn PC, s in g le IP ad d res s o r ran g e o f IP ad d res ses t h at are allo wed t o access t he GUI wit h HTTPS. W h en a n ext ern al SNM P man ag er is p ro v id ed wit h t h is ro u terâ□□s M anag emen t In fo rmat io n Bas e (M IB) file, t h e man ag er can u p d ate t he ro u terâ□□s h ierarch al v ariab les t o v iew o r u p d at e co n fig u rat io n p aramet ers . th e ro u ter as a man ag ed d evice h as an SNM P ag en t t h at allo ws t h e M IB co n fig u rat io n v ariab les t o b e acces s ed b y t h e M as t er (t h e SNM P man ag er). Th e A cces s Co n tro l Lis t o n t h e ro ut er id en tifies man ag ers in t h e n et wo rk t h at h av e read o n ly o r read -writ e SNM P cred en t ials . Select the routerâ□□s time zone, relative to Greenwich Mean Time (GMT).

Determine whether to use default or custom Network Time Protocol (NTP) servers. A s an ad min is t rat or y o u can mo n it o r t he t y pe o f t raffic t h at g o es t h rou gh t h e ro ut er an d als o b e n ot ified o f p o t en t ial at t acks o r erro rs wh en t h ey are d et ect ed b y t h e ro u t er. Th e fo llo win g s ect io n s d es crib e t h e lo g co n fig u rat io n s et t in g s an d t h e way s y o u can acces s t h es e lo g s . Fo r each facilit y , t h e fo llo win g ev en t s (in o rd er o f s ev erit y) can b e lo g g ed : Emerg en cy , A lert , Crit ical, Erro r , W arn in g , No t ificat io n , In fo rmat io n , Deb u g g in g . EM ERGENC Y: s y s t em is u n u s ab le A LERT: act io n mu s t b e t aken immed iat ely CRITICA L: crit ical co n d it io n s ERROR: erro r co n d it io n s W A RNING: warn in g co n d it io n s NOTIFICA TION: n o rmal b u t s ig n ifican t co n d it io n INFORM A TION: in fo rmat io n al DEBUGGIN G: d eb u g -lev el mes s ag es 163 Unified Services Router User Manual Figure 113 : Facility s e ttings for Logging Th e d is p lay fo r lo g g in g can b e cu st omized b as ed o n wh ere t h e lo g s are s en t , eit h er t h e Ev en t Lo g v iewer in t h e GUI (t h e Ev en t Lo g v iewer is in t h e Status > Logs p ag e) o r a remo t e Sy s lo g s erv er fo r lat er rev iew.

Den ial o f s erv ice at t acks , g en eral at t ack in fo rmat io n , lo g in at t emp t s , d ro p p ed p acket s , an d s imilar ev en t s can b e cap t u red fo r rev iew b y t h e IT ad min is t rat o r. Traffic t h ro u g h each n etwo rk s egmen t (LA N, W A N, DM Z) can b e t racked b as ed o n wh et h er t h e p acket was accep t ed o r d ro p p ed b y t h e firewall. A ccep t ed Packet s are t h o s e t h at were s u cces s fu lly t ran s ferred t h ro u g h t h e co rres p o n d in g n et wo rk s eg men t (i.) Dro p p ed Packet s are p acket s t hat were in t en tio nally b lo cked fro m b ein g t ran s ferred t h ro u g h t h e co rrespo ndin g n et work s eg men t. In ad d it io n t o n et work s egmen t lo g gin g, u n icast an d mu lt icast t raffic can b e lo g g ed .
165 Unified Services Router User Manual Figure 114 : Log configuratio n options for traffic through route r Tools > Log Settings > IPv6 logging Th is p ag e allo ws y o u t o co n fig u re t h e IPv 6 lo g g in g 166 Unified Services Router User Manual Figure 115 : IPv6 Log configuratio n options for traffi c through route r 9. Fo r remo t e lo g g in g a key co n fig u ration n field is t h e Remo t e Lo g Id en t ifier. Th e SM TP p o rt an d ret u rn e -mail ad d res ses are req u ired field s t o allo w t h e ro u ter t o p ackage t he lo g s an d s end a v alid e-mail t h at is accep ted b y o ne o f t h e co nfig ured â□□s end -to â□□ ad dress es . Up t o t h ree e mail ad d res s es can b e co n fig u red as lo g recip ien t s . in o rd er t o es t ablis h a co n n ection wit h t h e co nfig ured SM TP p o rt an d s erv er , d efin e t h e s erv erâ□□s au t h en t icat io n req u iremen t s . Th e ro u t er s u p p o rt s Lo g in Plain (n o en cry p t ion) o r CRA M -M D5 (en cry p ted) fo r t h e u s ern ame an d p as s wo rd d at a t o b e s en t t o t h e SM TP s erv er. a u th en ticat io n can b e d is ab led if t h e s erv er d o es n o t h av e t h is req u iremen t . In s ome cas es t h e SM TP s erver may s en d o u t IDENT req u es ts, an d t h is ro u t er can h av e t h is res p o n s e o p t io n en ab led as n eed e d . On ce t h e e -mail s erv er an d recip ient d etails are d efin ed y o u can d etermin e wh en t h e ro u t er s h ou ld s end o ut lo g s. Th is remo t e d evice t y pically h as les s memo ry co n s t rain t s t h an t h e lo cal Ev en t Viewer o n t h e ro u t erâ□□s GUI, an d t h u s can co llect a co n s id erab le n u mb er o f lo g s o v er a s u stain ed p eriod .

To en able a Sy s lo g s erver s elect t h e ch eckbo x n ext t o an emp t y Sy s lo g s erver field an d assig n t h e IP ad d ress or FQDN t o t h e Name field . th e s elect ed facilit y an d s ev erit y lev el mes s ag es will b e 168 Unified Services Router User Manual s en t t o t h e co nfig u red (an d en abled) S y s log server o n ce y o u s av e t h is co n fig u rat io n p ag eâ□□s s et t in g s . Figure 117 : Sys log s e rve r configuratio n for Re mote Logging (continue d) 9. W h en ev er t raffic t h ro u g h o r t o t h e ro u t er mat ch es t h e s et t in g s d et ermin ed in t h e Tools > Log Settings > Logs Facility o r Tools > Log Settings > Logs Configuration p ag es , t h e co rres p o n d in g lo g mes s ag e will b e d is p lay ed in t h is win d o w wit h a t imes t amp . 5 Backing up and Restoring Configuration Settings Tools > System Yo u can b ack u p t h e ro u t erâ□□s cu s t o m co n fig u rat io n s et t in g s t o res t o re t h em t o a d ifferen t d ev ice o r t h e s ame ro u t er aft er s o me o t h er ch an g es . On ce t h e LEDs are t u rn ed o ff, wait a few mo re s eco n d s b efo re d o in g an y t h in g wit h t h e ro u t er. fo r b ackin g u p co nfig u rat io n o r res t o rin g a p rev io u s ly s av ed co n fig u rat io n , p leas e fo llo w t h e s t ep s b elo w: 1. To save a copy of your current settings, click the Backup button in the Save Current Settings option. The browser initiates an export of the configuration file and prompts to save the file on your host. 170 Unified Services Router User Manual 2.
To restore your saved settings from a backup file, click Browse then locate the file on the host. After clicking Restore, the router begins importing the fileâ□□s saved configuration settings. After the restore, the router reboots automatically with the restored settings. 3. To erase your current settings and revert to factory default settings, click the Default button.
The router will then restore configuration settings to factory defaults and will reboot automatically. (See Appendix B for the factory default parameters for the router). Figure 119 : Re s toring configuratio n from a s ave d file will re s ult in the curre nt configurat io n be ing ove rwritte n and a re boot 9. Ho wev er, all u s er d at ab as es will b e s wep t away wh en u sers d own grade firmware fro m 1. 7 Upgrading Router Firmware via USB Tools > Firmware via USB Th is p ag e allo ws u ser t o u pg rad e t h e firmware, b acku p an d rest ore t he s et tin gs u sing a USB s t o rag e key .
Each co n fig u red W A N can h av e a d ifferen t DDNS s erv ice if req u ired . on ce co n fig u red , t h e ro u ter will u p d at e DDNS s erv ices ch an ges in t h e W A N IP ad d res s s o t h at feat u res t h at are d ep en d en t o n acces s in g t h e ro u t erâ□□s W A N v ia FQDN will b e d irect ed t o t h e co rrect IP ad d ress. W hen y o u s et u p an acco u n t wit h a DDNS s erv ice, t h e h o s t an d d o main n ame, u s ername, p asswo rd an d wild card s u ppo rt will b e p ro v id ed b y t h e acco u n t p ro v id er. 1 Ping Th is u t ilit y can b e u s ed t o t est co n nect ivit y b et ween t h is ro u t er an d an o t h er d ev ice o n t h e n et wo rk co n n ect ed t o t h is ro u t er. 4 Router Options Th e s t at ic an d d y namic ro u t es co n fig u red o n t h i s ro u t er can b e s h o wn b y clickin g Dis p lay fo r t h e co rres po n d in g ro u t in g t ab le. Th e s et t in g s fo r t h e wired an d wireles s in t erfaces are d is p lay ed in t h e DSR St at u s p ag e, an d t h en t h e res u lt in g h ard ware res o u rce an d ro u t er u s ag e d et ails are s u mmarized o n t h e ro u t erâ□□s Das h b o ard . Th e ra d io b and an d ch annel s ett in g s are p res en t ed b elo w alo n g wit h all co n fig u red an d act iv e A Ps t h at are en ab led o n t h is ro u t er. 1 W ired Port Statistics Status > Traffic Monitor > Device Statistics Det ailed t ran s mit an d receiv e s t at is t ics fo r each p h y s ical p o rt are p res en t ed h ere. each in t erface (W A N1 , W A N2/ DM Z , LA N , an d VLA Ns) h av e p o rt s p ecific p acket lev el in fo rmat io n p ro v id ed fo r rev iew. Tran s mit t ed/receiv ed p acket s, p ort co llis ions, an d t h e cu mu lat in g b y tes/sec fo r t ran s mit / receiv e d irect io n s are p ro v id ed fo r each in t erface alo n g wit h t h e p o rt u p t ime.